Configuration Guide

hp StorageWorks Data Replication Manager HSG80 ACS Version 8.7P

Product Version: ACS v8.7P

Sixth Edition (March 2004)

Part Number: AA–RPHZF–TE

HP StorageWorks Data Replication Manager provides a disaster-tolerant solution for secure data storage through the use of hardware redundancy across several sites. Multiple heterogeneous servers can be connected to one or more shared storage subsystems. This document provides instructions for configuring a Data Replication Manager solution and verifying the validity of the configuration.

For the latest version of this guide and other Data Replication Manager documentation, access the website at http://h18000.www1.hp.com/products/sanworks/drm/index.html. Click the **technical documentation** link and the technical support page is displayed. Click **manuals (guides, supplements, addendums, etc)** for a listing of related documentation.

Data Replication Manager
HSG80 ACS Version 8.7P Configuration Guide
Sixth Edition (March 2004)
Part Number: AA–RPHZF–TE

contents

About this Guide . . . 13
Overview . . . 14
Intended Audience . . . 14
Related Documentation . . . 14
Conventions . . . 15
Document Conventions . . . 15
Text Symbols . . . 15
Equipment Symbols . . . 16
Rack Stability . . . 17
Getting Help . . . 17
HP Technical Support . . . 17
HP Storage Web Site . . . 17
HP Authorized Reseller . . . 18

1 Introduction to Data Replication Manager . . . 19
Data Replication Manager Overview . . . 20
Heterogeneous Storage Area Networks . . . 20
Required Hardware Components . . . 21
Rack Components . . . 21
ESA12000 Storage Rack . . . 22
EMA12000 Modular Storage Rack . . . 24
Fibre Channel Switches . . . 25
Gigabit Interface Converters . . . 27
Power Distribution Unit . . . 27
Fully-Redundant Power (Optional) . . . 27
Host Bus Adapters . . . 27
Hardware Configurations . . . 28
Software Components . . . 30
Array Controller Software . . . 30
Secure Path . . . 30
Control and Monitoring Tools . . . 30
StorageWorks Command Console (Optional) . . . 31
Restrictions . . . 31

2 Remote Copy Set Features . . . 33
Remote Copy . . . 34
Remote Copy Sets . . . 34

Nonremote Copy Sets 34
Operation Modes 34
Synchronous Operation Mode 34
Asynchronous Operation Mode 34
Operation Mode Considerations 35
ADD REMOTE_COPY_SETS Command 35
Outstanding_IO Settings 35
Synchronous 36
Asynchronous 36
Outstanding Write Operations 36
High Outstanding I/O Values 36
Low Outstanding I/O Values 36
Suspend and Resume Switches 36
Error Mode Switch 37
Association Sets 37
Association Set Characteristics 37
FAIL_ALL Switch 38
ADD ASSOCIATIONS Command 39
Write History Logging 39
Write History Log Units 39
Write History Log Unit Restrictions 40
Reaching the End of a Write History Log Unit 40
Write History Log Unit Performance Considerations 41
Write History Log Unit Size Considerations 41
Switches 41
Write History Log Unit Switches 41
ORDER_ALL Switch 42
SUSPEND 42
RESUME 42
Failover 42
Planned Failover 42
Unplanned Failover 43
Failback 43

3 Getting Started 45
Site, Host, and Solution Preparation 46
Host Bus Adapter Requirements 46
Setting Up the B-Series Fibre Channel Switches 46
Setting Up the Fiber Optic Cables 47
Host-to-Switch Connections 48
Switch-to-Controller Connections 48
Changing SCSI Version from SCSI-2 to SCSI-3 on HSG80 Controllers 49
Static Upgrade Procedure 49
Rolling Upgrade Procedure 52
Cascaded Switches 52
Hopping 52
Cascaded Switch Configurations 53
Multiple Intersite Links 55

4 Configuring a Standard Data Replication Manager Solution 57
Introduction. 58
Restrictions. 58
Configuration Overview 60
Configuration Procedures Outline 60
Target Site Outline. 60
Initiator Site Outline 61
Configure the Controllers at the Target Site. 62
Configure Storage at the Target Site 69
Devices and Storagesets. 69
Create Storage Units 69
Cable the Target Site 71
Connect Fiber Optic Cables Between Controllers and Fibre Channel Switches 71
Connect the Target Site to the External Fiber Link 73
LongWave or Very Long Distance GBICs 73
Other Transport Modes 73
Create Switch Zones at the Target Site. 74
Configure the Host at the Target Site 74
HP OpenVMS 74
Install the HBAs 74
Install SWCC (Optional) 75
Additional Setup 75
Connect the Host to the SAN 75
Rename the Host Connections. 75
Update Switch Zones. 77
HP Tru64 UNIX. 77
Install the HBAs 77
Install the HBA Driver 77
Multipath Software 78
Install SWCC (Optional) 78
Connect the Host to the SAN 78
Rename the Host Connections. 78
Update Switch Zones. 79
HP-UX 80
Existing Fibre Channel HP-UX Configurations 80
Install the HBAs 80
Connect the Host to the SAN 80
Rename the Host Connections. 80
Update Switch Zones. 81
Disable Access to the Hosts at the Target Site 81
Install the Secure Path Fibre Channel HBA Device Driver 81
Verify the Disks. 81
Configure the SWCC Agent (Optional) 82
Additional Setup 82
IBM AIX 82
Install the HBAs 82
Install the Secure Path Fibre Channel HBA Device Driver and the AIX Platform Kit 83
New Installation 83
New Installation Assumptions 83
HBA Limitations 83

Installation Steps 83
Upgrade Installation 85
Upgrade Installation Assumptions 85
HBA Limitations 85
Installation Steps 85
Connect the Host to the SAN 88
Rename the Host Connections 88
Update Switch Zones 89
Disable Access to the Hosts at the Target Site 89
Verify the Disks 89
Configure the SWCC Agent (Optional) 90
Additional Setup 90
Microsoft Windows NT and Windows 2000 90
Install the HBAs and Update Firmware 90
Install the HBA Driver 90
Install Fibre Channel Software 90
Install Multipath Software 91
Install SWCC (Optional) 91
Connect the Host to the SAN 91
Rename the Host Connections 92
Update Switch Zones 93
Novell NetWare 93
Install the HBAs 93
Install the HBA Driver 93
Install Secure Path Agent 93
Install Secure Path Manager 94
Install SWCC (Optional) 94
Connect the Host to the SAN 94
Rename the Host Connections 95
Update Switch Zones 96
Sun Solaris 96
Install the HBAs 96
Connect the Host to the SAN 97
Install the Solaris Platform Kit 97
Rename the Host Connections 98
Update Switch Zones 98
Enable Access to the Hosts at the Target Site 99
Verify the Disks 99
Install Secure Path for Solaris Software 99
Reverify the Disks 99
Configure SWCC Agent (Optional) 99
Disable Access to the Hosts at the Target Site 100
Additional Setup 100
Configure the Controllers at the Initiator Site 100
Configure Storage at the Initiator Site 107
Devices and Storagesets 107
Create Storage Units 107
Cable the Initiator Site 109
Connect Fiber Optic Cables Between Controllers and Fibre Channel Switches 109
Connect the Initiator Site to the External Fiber Link 111

Longwave or Very Long Distance GBICs 111
Other Transport Modes 111
Create Switch Zones 112
Create Remote Copy Sets 112
Prepare the Initiator Site 112
Create Connections from the Target Site 112
Create Remote Copy Sets from the Initiator Site 113
Set Failsafe at the Initiator Site (Optional) 114
Create Write History Log Units and Association Sets (Optional) 115
Create a Write History Log Unit 115
Create Association Sets and Assign a Write History Log Unit 116
Configure the Host at the Initiator Site 118
HP OpenVMS 118
Install the HBAs 118
Install SWCC (Optional) 118
Additional Setup 119
Connect the Host to the SAN 119
Rename the Host Connections 119
Update Switch Zones 120
Enable Access to the Hosts at the Initiator Site 120
HP Tru64 UNIX 121
Install the HBAs 121
Install the HBA Driver 121
Multipath Software 121
Install SWCC (Optional) 121
Connect the Host to the SAN 121
Rename the Host Connections 122
Update Switch Zones 123
Enable Access to the Hosts at the Initiator Site 123
HP-UX 123
Existing Fibre Channel HP-UX Configurations 124
Install the HBAs 124
Connect the Host to the SAN 124
Rename the Host Connections 124
Update Switch Zones 125
Enable Access to the Hosts at the Initiator Site 125
Install the Secure Path Fibre Channel HBA Device Driver 125
Verify the Disks 125
Configure the SWCC Agent (Optional) 126
Additional Setup 126
IBM AIX 126
Install the HBAs 126
Install the Secure Path Fibre Channel HBA Driver and the AIX Platform Kit 126
New Installation 126
New Installation Assumptions 126
HBA Limitations 127
Installation Steps 127
Upgrade Installation 129
Upgrade Installation Assumptions 129
HBA Limitations 129

Installation Steps 129
Connect the Host to the SAN 132
Rename the Host Connections 132
Update Switch Zones 132
Enable Access to the Hosts at the Initiator Site 133
Verify the Disks 133
Configure the SWCC Agent (Optional) 133
Additional Setup 133
Microsoft Windows NT and Windows 2000 134
Install the HBAs 134
Install the HBA Driver 134
Install Fibre Channel Software 134
Install Multipath Software 134
Install SWCC (Optional) 135
Connect the Host to the SAN 135
Rename the Host Connections 135
Update Switch Zones 136
Novell NetWare 137
Install the HBAs 137
Install the HBA Driver 137
Install Secure Path Agent 137
Install Secure Path Manager 138
Install SWCC (Optional) 138
Connect the Host to the SAN 138
Rename the Host Connections 139
Update Switch Zones 140
Enable Access to the Hosts at the Initiator Site 140
Sun Solaris 141
Install the HBAs 141
Connect the Host to the SAN 141
Install the Solaris Platform Kit 141
Rename the Host Connections 142
Update Switch Zones 143
Enable Access to the Hosts at the Initiator Site 143
Verify the Disks 143
Install Secure Path for Solaris Software 143
Reverify the Disks 144
Configure the SWCC Agent (Optional) 144
Additional Setup 144
Additional Host Configuration 144
Install Cluster Server for Windows NT and Windows 2000 (Optional) 144
Install NetWare Cluster Services (NWCS) Version 1.01 (Optional) 144
Documenting Your Configuration 145
Terminal Emulator Session 145
SHOW Commands 145

5 Configuring the Optional Entry-Level DRM Solutions 149
Overview 149
Dual-Switch Single-Site Configuration 150
Setting Up the Dual-Switch Single-Site DRM Configuration 151

Single-Switch Configuration 152
Setting Up the Single-Switch Configuration 153
Single-Fabric Configuration 154
Setting Up the Single-Fabric Configuration 156

6 Configuring the Optional Advanced DRM Solutions 159
Bidirectional DRM Solution 159
Stretched Cluster DRM Solution 160

7 Troubleshooting 161
Preliminary Checks 162
Information from the Controllers 162
Step 1: Issue a SHOW THIS Command 162
Step 2: Issue a SHOW OTHER Command 164
Step 3: Issue a SHOW CONNECTIONS Command 165
Information from the Switches 167
Step 4: Issue switchShow Command from the First Switch 168
Step 5: Issue switchShow Command from the Second Switch 169
Step 6: Issue switchShow Command from the Third Switch 171
Step 7: Issue switchShow Command from the Fourth Switch 173
Information from the Operating Systems 175
Step 8: Associating HBAs with Servers 175
HP OpenVMS 175
HP Tru64 UNIX 176
HP-UX 176
IBM AIX 176
Microsoft Windows NT and Windows 2000 177
Novell NetWare 177
Sun Solaris 177
Other Troubleshooting Considerations 179
SHOW Commands 179
SHOW UNITS FULL 179
SHOW REMOTE FULL 179
Zoning 180
Secure Path 180
Controller Replacement in a DRM Configuration 181

8 Zoning in the Storage Area Network 183
Switch Zoning 184
Planning Considerations for Homogeneous and Heterogeneous Configurations That Require Zoning 184
More than 96 Host Connections 184
Zoning Hosts and HSG80 Subsystems Between Sites 185
Zoning a DRM Configuration 185
DRM Homogeneous Configuration 185
Example: Zoning Green Zone_Top and Green Zone_Bottom 189
Example: Zoning Blue Zone_Top and Blue Zone_Bottom 191
Example: Zoning Red Zone_Top and Red Zone_Bottom 193
Create the Zone Names 196
Create the Configuration Name 196
DRM Heterogeneous Configuration 197

Example: Zoning Yellow Zone_Top and Yellow Zone_Bottom 200
Example: Zoning Brown Zone_Top and Brown Zone_Bottom 202
Create the Zone Names 204
Add the New Zones to the Configuration 204
Zoning to Allow Host Access Between Sites 208

A Status Comparison 211
Target Site Terminal Emulator Session 212
Issuing SHOW Commands 212

B Replicating Storage Units 215
Cloning Data for Backup 217
Snapshot 219
Snapshot Command 220

C Upgrading to ACS Version 8.7P Software 223
Rolling Upgrade Procedure for Version 8.6-xP to 8.7P 224
Initiator Site Upgrade Procedure 224
Target Site Upgrade Procedure 228
Completion of the Initiator Site Upgrade Procedure 231
Shutdown Upgrade Procedure for 8.7P 231
Initiator Site Shutdown Upgrade Procedure 231
Target Site Shutdown Upgrade Procedure 234
Completion of Initiator Site Shutdown Upgrade Procedure 236

Glossary 237

Index 251

Figures

1 ESA12000 SBB units 22
2 Additional components for ESA12000 Data Replication Manager 23
3 Components of EMA12000 modular storage for Data Replication Manager 25
4 Fibre Channel SAN Switch 16 26
5 Fibre Channel SAN Switch 8-EL 26
6 StorageWorks edge switch 2/16 26
7 StorageWorks director 2/64 26
8 Fibre Channel-based ESA12000 DT storage subsystem (with fully-redundant power) 28
9 Fibre Channel-based EMA12000 DT modular storage subsystem (with fully-redundant power) 29
10 Remote copy set operation modes 35
11 Location of association sets on the initiator dual controller 38
12 Locations and names of components for connecting fiber optic lines 47
13 Cascaded switches in a DRM environment 53
14 Cascaded switches in DRM environment with three hops between host and controller 54
15 Multiple intersite links 55
16 Basic Data Replication Manager configuration 58
17 Cabling between the controllers and the Fibre Channel switches 72
18 Cabling from the target site to the initiator site 73
19 Host renaming worksheet 76
20 Cabling between the controllers and the Fibre Channel switches 110

21 Cabling from the initiator to the target site 111
22 DRM dual-switch single-site configuration 150
23 Single-switch DRM configuration 153
24 Dual switch with single ISL 155
25 Bidirectional DRM configuration 160
26 Controller pair World Wide IDs 164
27 First cabling diagram 169
28 Second cabling diagram 171
29 Third cabling diagram 173
30 Fourth cabling diagram 175
31 Final configuration 178
32 Zoning in a DRM homogeneous environment 186
33 Zoning a DRM example 188
34 Zoning in a DRM heterogeneous environment 198
35 DRM example showing the new zones 199
36 Steps the CLONE utility follows for duplicating unit members 217
37 Snapshot unit 219
38 Controller reset button and first three LEDs 226

Tables

1 Document conventions 15
2 ESA12000 Storage Rack Components 22
3 EMA12000 Modular Storage Rack Components 24
4 Controller Option Settings for DRM 44
5 Example of Wiring for First Server and First Storage Array at Each Site 49
6 Restrictions and Requirements 58
7 Comparison of Entry-Level Configurations 149
8 SHOW THIS Command Analysis 163
9 SHOW OTHER Command Analysis 164
10 SHOW CONNECTIONS Command Analysis 166
11 Switch Version Command 167
12 First switchShow Command Output 168
13 Second switchShow Command Output 170
14 Third switchShow Command Output 172
15 Fourth switchShow Command Output 174
16 SHOW UNITS FULL Command Output 179
17 SHOW REMOTE FULL Command Output 180
18 Blank zoning input form template 187
19 Green Zone_Top and Green Zone_Bottom input form 189
20 Blue Zone_Top and Blue Zone_Bottom input form 192
21 Red Zone_Top and Red Zone_Bottom input form 194
22 Yellow Zone_Top and Yellow Zone_Bottom input form 200
23 Brown Zone_Top and Brown Zone_Bottom input form 203
24 Cloning and Snapshot Comparison 215

About This Guide

This configuration guide provides information to help you:

- Understand HP StorageWorks Data Replication Manager (DRM) hardware requirements and configurations
- Understand remote copy set concepts
- Set up and cable your DRM solutions
- Consider entry-level and advanced configurations
- Troubleshoot your DRM configuration
- Decide how zoning will help your DRM configuration
- Contact technical support for additional assistance

This configuration guide contains minor edits since the last edition, consisting mostly of changes in links and references, and was also reformatted to meet newer company standards.

"About this Guide" topics include:

- Overview, page 14
- Conventions, page 15
- Rack Stability, page 17
- Getting Help, page 17

Overview

This section covers the following topics:

- Intended Audience
- Related Documentation

Intended Audience

This book is intended for use by system administrators who are experienced with the following:

- ACS Version 8.7P for their DRM storage system
- Administration of the various operating systems used by the hosts in their heterogeneous SAN

Related Documentation

In addition to this guide, HP provides additional information you may need to reference when connecting, configuring, and operating your DRM solution:

- *HP StorageWorks Data Replication Manager HSG80 Version 8.7P Failover/Failback Procedures Guide*, part number AA-RPJ0E-TE
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Release Notes*, part number AA-RPJ2E-TE
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Scripting User Guide*, part number EK-DRMSC-OA. E01
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Design Guide Application Notes*, part number AA-RQ78C-TE
- *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide*, part number AA-RU5CE-TE
- *HP StorageWorks SAN Design Reference Guide*, part number AA-RMPNL-TE
- *HP StorageWorks HSG80 Array Controller ACS Version 8.7 CLI Reference Guide*, part number EK-G80CL-RA. B01
- *HP StorageWorks HSG80 Array Controller ACS Version 8.7 Maintenance and Service Guide*, part number EK-G80MS-SA. B01
- *HP StorageWorks HSG60 and HSG80 Controller and HSx80 Cache Module Replacement Procedures for Array Controller Software V8.7x-x Release Notes,* part number AA-RUQ2A-TE
- *Compaq StorageWorks Command Console Version 2.4 User Guide*, part number AA-RFA2H-TE
- *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide*, part number AA-RKPDB-TE

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

This document follows the conventions in Table 1.

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

▷ Identifies a procedural step to be performed at the initiator site.

⊙ Identifies a procedural step to be performed at the target site.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

Introduction to Data Replication Manager

1

This chapter introduces HP StorageWorks Data Replication Manager (DRM) and describes the required hardware and software components.

This chapter covers the following:

- Data Replication Manager Overview, page 20
- Heterogeneous Storage Area Networks, page 20
- Required Hardware Components, page 21
  - Rack Components, page 21
  - ESA12000 Storage Rack, page 22
  - EMA12000 Modular Storage Rack, page 24
  - Fibre Channel Switches, page 25
  - Gigabit Interface Converters, page 27
  - Power Distribution Unit, page 27
  - Fully-Redundant Power (Optional), page 27
  - Host Bus Adapters, page 27
- Hardware Configurations, page 28
- Software Components, page 30
  - Array Controller Software, page 30
  - Secure Path, page 30
  - Control and Monitoring Tools, page 30
  - StorageWorks Command Console (Optional), page 31

Data Replication Manager Overview

DRM provides a disaster-tolerant (DT) storage solution through the use of hardware redundancy and data replication between two sites separated by some distance. Multiple heterogeneous servers can be connected to one or more shared storage subsystems.

A basic DRM configuration consists of two sites—an *initiator* and a *target*. The initiator site carries out primary data processing. The target site is used for data replication. As data processing occurs at the initiator site, the data is replicated or mirrored to the target site. If a single component at either site fails, DRM will fail over to a redundant component at the same site to allow continued operation. For example, if one of the dual-redundant Fibre Channel links between the sites were to fail, DRM would fail over to the other link. If a significant failure (disaster) occurs at the initiator site, data processing can be resumed at the target site, where the data is intact. This process is called *site failover.* When the cause of the initiator site failover has been resolved, data processing can be moved back to the initiator site in a process called *site failback*.

DRM uses the peer-to-peer remote copy function of the HSG80 controller to achieve data replication. HSG80 controller pairs at the initiator site are connected to their partner HSG80 controller pairs at the target site. This process is completely host independent.

The connection between the two DRM sites is called an *intersite link* (ISL). There are two ISLs for redundancy. An ISL can be one of several transport modes. For example, short distances can use direct Fibre Channel links, but longer distances may require asynchronous transport mode (ATM). For more detailed information on supported ISLs, refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide* and to the most recent DRM Release Notes for any support information related to your operating system.

Heterogeneous Storage Area Networks

This section describes heterogeneous storage area networks (SANs) in a DRM environment. Previous implementations of DRM required all operating systems in a DRM environment to be the same (homogeneous). The latest version of the Array Controller Software (ACS) supports a mixed (heterogeneous) environment of operating systems, making DRM much more scalable and manageable in a customer data center.

SANs are becoming more complicated to manage and maintain. In today's Information Technology world, few businesses carry out their day-to-day operations within a single operating system (OS) topology. Many businesses have a mixture of operating system platforms carrying out different business functions. They may have electronic mail services running on Windows 2000, critical business applications on UNIX, and file-print services on NetWare. These may be running in several data centers on several different SANs. By using a heterogeneous DRM SAN environment, they can be combined into a single SAN and use a single implementation of DRM for business critical applications.

Refer to the *HP StorageWorks SAN Design Reference Guide* for more information on designing and building heterogeneous SANs. If the *HP StorageWorks SAN Design Reference Guide* contradicts this guide, consider this guide correct for DRM configurations only.

Required Hardware Components

DRM uses a minimum of two HSG80 Array Controller pairs: one at the initiator site and one at the target site. Each site must have one or more ESA12000 racks or EMA12000/EMA16000 modular storage racks:

- RA8000/ESA12000 racks are equipped with one or more BA370 enclosures and disk storage building blocks (SBBs). Each BA370 enclosure holds up to 24 disks.
- MA8000/EMA12000/EMA16000 modular storage racks are equipped with one or more controllers and modular disk SBBs.

The hosts at the initiator and target sites are connected to a pair of dual-redundant HSG80 Array Controllers, which are located inside the enclosures. Connections between the controllers and hosts are made at each site with two Fibre Channel switches and two host bus adapters (HBAs). For complete details on this equipment, refer to the storage rack installation reference guide for your operating system.

Note: Although this documentation addresses ESA12000 storage racks as a primary unit for DRM configurations, the HP DT solution functions in any equivalent rack that houses a BA370 enclosure. For the EMA12000/EMA16000 modular storage racks, the HP DT solution functions in any equivalent rack that houses the same number of controllers and an equivalent drive configuration. Rack configurations may also be combined between the ESA12000 racks and EMA12000/EMA16000 modular storage racks. For example, if the disk configurations are equivalent, an ESA12000 rack may be used at one site (initiator or target) and an EMA12000/EMA16000 modular storage rack may be used at the associated site (target or initiator).

Rack Components

Tables and figures throughout this chapter show hardware that is necessary or optional to complete a modular DRM solution for each of two types of rack configurations, the ESA12000 rack and the EMA12000/EMA16000 modular storage rack.

For detailed information about these components, refer to the following documents:

- The HP StorageWorks HSG80 ACS Solution Software Version 8.7P for your operating system
- *HP StorageWorks HSG80 Array Controller ACS Version 8.7 CLI Reference Guide*
- *HP StorageWorks HSG80 Array Controller ACS Version 8.7 Maintenance and Service Guide*

ESA12000 Storage Rack

The ESA12000 SBB rack houses the BA370 enclosures, which contain the components listed in Table 2.

Table 2: ESA12000 Storage Rack Components

Two HSG80 Fibre Channel RAID array controllers
One Environmental Monitoring Unit (EMU)
One or two AC input power controllers
Up to 24 disk drive SBBs per BA370 enclosure
Five to eight 180-watt power supplies
Dual external cache batteries (ECBs)
Six single-ended I/O Ultra SCSI modules
Eight cooling fans
One Power Verification and Addressing (PVA) module
Two cache modules (512 MB each required) for each HSG80

Figure 1 shows the initial SBB parts inside the ESA12000 rack with a 24 disk-drive capacity.

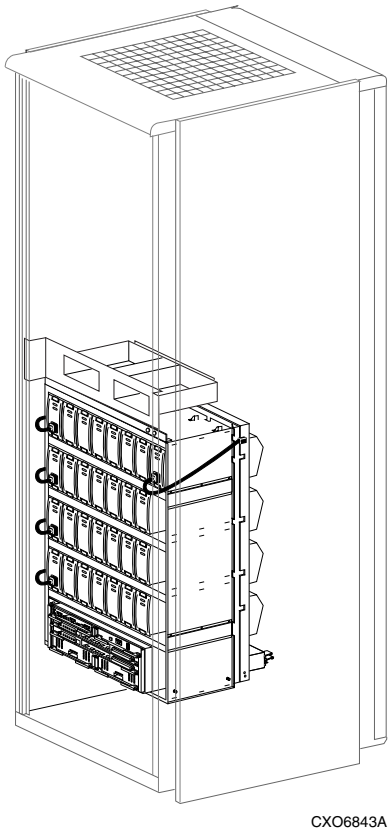


Figure 1: ESA12000 SBB units

Figure 2 shows additional components that must be added to the ESA12000 building block to support a DRM solution, including Fibre Channel switches. The optional redundant power distribution unit is also shown.

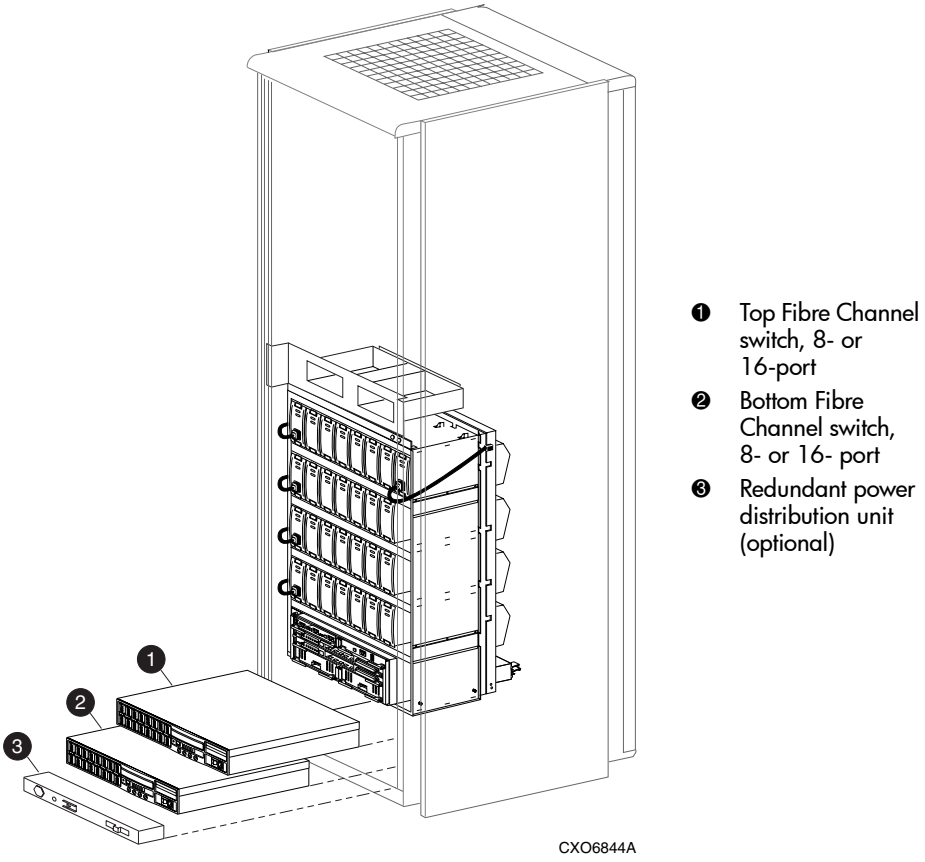


Figure 2: Additional components for ESA12000 Data Replication Manager

EMA12000 Modular Storage Rack

The EMA12000 modular SBB racks include power distribution units, are pre-cabled, and contain the components listed in Table 3.

Table 3: EMA12000 Modular Storage Rack Components

Two HSG80 Fibre Channel RAID array controllers
Two Environmental Monitoring Units (EMUs)
Two AC input power controllers
Modular disk drive SBBs:
D14—Up to 42 drives per controller subsystem
S14 —Up to 72 drives per controller subsystem
Blue—Up to 42 drives per controller subsystem
Dual power supplies, one set per enclosure
Dual external cache batteries (ECBs)
Dual cooling fans, one set per enclosure
Six single-ended I/O Ultra SCSI modules
Two cache modules (512 MB each required)

Figure 3 shows an EMA12000 modular building block that supports a DRM solution. The modular SBB consists of the controller enclosure and the disk enclosure. The redundant power distribution unit is also shown.

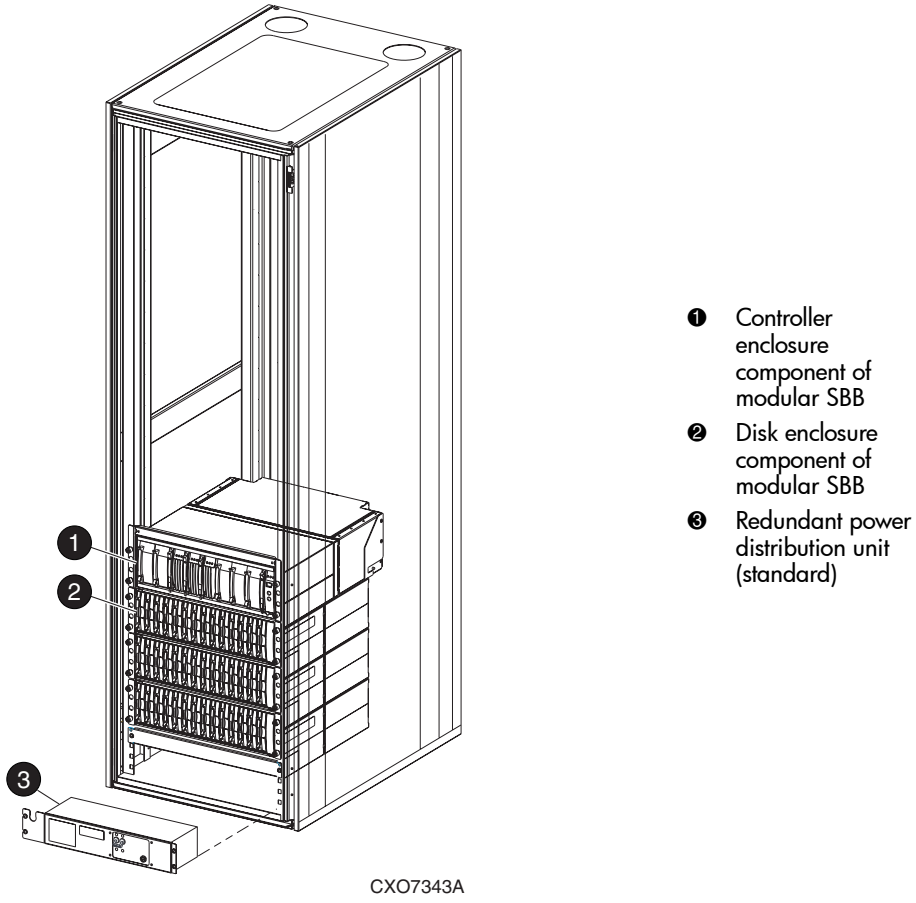


Figure 3: Components of EMA12000 modular storage for Data Replication Manager

Switches are placed in a different rack in this configuration of the EMA12000 D14 high-performance modular storage rack. A command center rack can be used to contain the switches.

Fibre Channel Switches

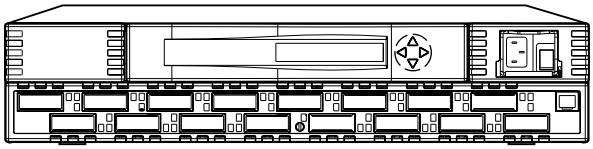
The Fibre Channel switches shown in Figure 4 through Figure 7 illustrate four models of SAN switches used to connect the controllers to the hosts and to link the initiator and target sites together. Three switch product lines are supported with DRM:

- B-series switches
- C-series switches
- M-series switches

The ports hold shortwave, longwave, or very long distance gigabit interface converters (GBICs), which are described in the next section.

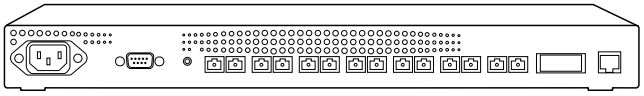
Refer to the HP Infrastructure website for additional information on supported switches at:

http://h18006.www1.hp.com/storage/saninfrastructure.html



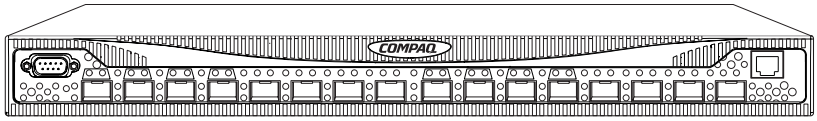
CXO7085A

Figure 4: Fibre Channel SAN Switch 16



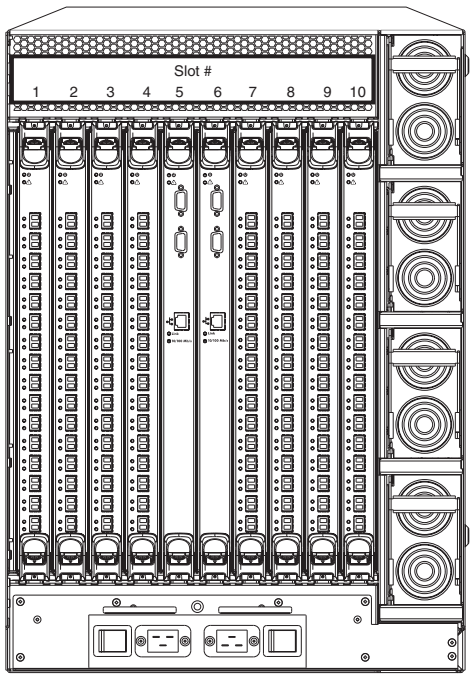
CXO7337A

Figure 5: Fibre Channel SAN Switch 8-EL



CXO7977A

Figure 6: StorageWorks edge switch 2/16



CXO7978A

Figure 7: StorageWorks director 2/64

Gigabit Interface Converters

Gigabit interface converters (GBICs) are the converters that are inserted into the ports of the Fibre Channel switch to serve as the interface between the fiber optic cables and the switch. Short-wave GBICs are used with a 50-micron multimode fiber optic cable (SC-terminated) to connect the components at the initiator and target sites (host-to-switch; controller-to-switch). The maximum distance that short-wave GBICs support is 500 meters.

Long-wave GBICs are used with 9-micron single-mode fiber optic cables (SC-terminated) to link the initiator and target sites. Standard long-wave GBICs connect switches that are up to 10 kilometers apart.

Very long distance GBICs are used with 9-micron single-mode fiber optic cables (SC-terminated) to link the initiator and target sites. Standard very long distance GBICs connect switches that are up to 100 kilometers apart.

Refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide* to learn more about GBICs.

Power Distribution Unit

The power distribution unit (PDU) component is included with the ESA12000 and EMA12000 racks:

- For the RA8000/ESA12000 racks, the PDU distributes power to the BA370s and switches. You can order a second PDU to support a fully-redundant MA8000/ESA12000 power configuration.
- For the RA8000/EMA12000 racks, the PDU distributes power to the modular configurations of controllers. PDU redundancy is included with MA8000/ESA12000 modular configurations.

Fully-Redundant Power (Optional)

Fully-redundant power is an optional feature designed to offer a more secure source of power in case one or more units fail. If fewer than five power components are operational, the entire rack shuts down.

The fully-redundant power feature requires three additional power supplies, as well as one additional AC power controller that plugs into one additional PDU. For the ESA12000 rack, these additional components must be supplied for each BA370 enclosure. For the EMA12000 modular storage rack, the preconfiguration models (D14, S14, Blue) feature fully-redundant enclosures.

Host Bus Adapters

The HBAs are inserted into the available slots on the host computer's PCI bus. A Fibre Channel connection is made by inserting a multimode fiber optic cable between each adapter and an individual port on the Fibre Channel switch.

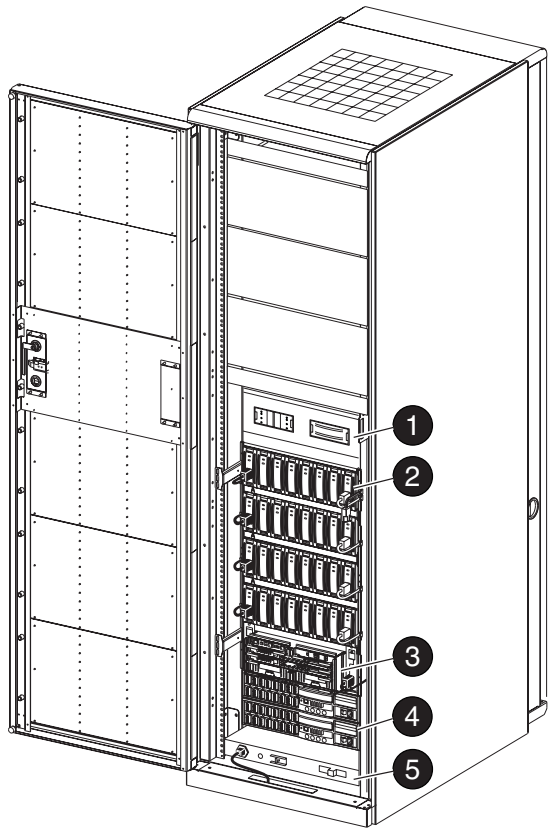
For a list of the most current software, firmware, patches, drivers, and so on, for each of the supported operating systems in your DRM solution, refer to the DRM Release Notes.

Hardware Configurations

Figures shown previously in this chapter have reflected the build of a DT solution for each of two types of rack configurations. Figure 8 shows a completed DT setup for the ESA12000 rack. Figure 9 shows a completed DT setup for the EMA12000 modular storage rack.

Note: If you prefer to join racks for more storage capacity, follow the instructions in the rack documents.

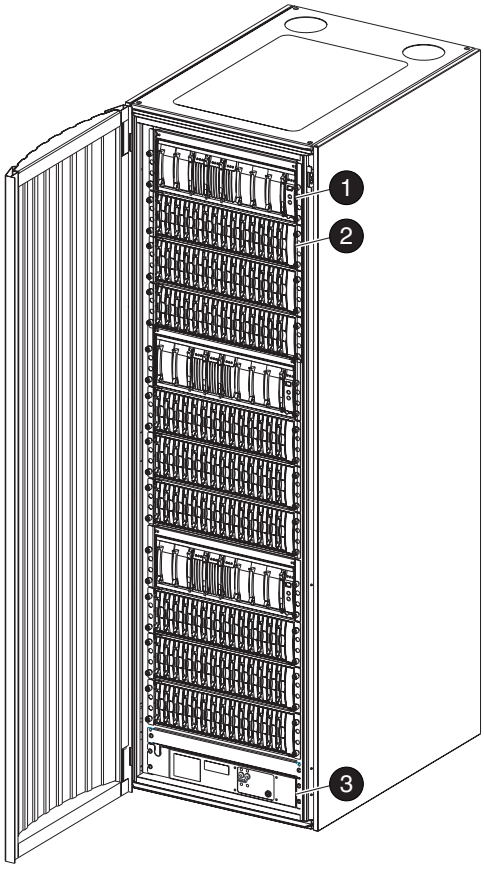
Be sure to establish the same setup at both the initiator and target sites. Keep in mind that an additional rack will not include switches or controllers. It does, however, include a PDU and is able to support redundant power.



❶ Cache battery
❷ SBBs
❸ Controllers
❹ Fibre Channel switches, 8- or 16 port
❺ Redundant power distribution unit

CXO7433A

Figure 8: Fibre Channel-based ESA12000 DT storage subsystem (with fully-redundant power)



❶ Controller enclosure component of modular SBB

❷ Disk enclosure component of modular SBB

❸ Redundant power distribution unit (standard)

Figure 9: Fibre Channel-based EMA12000 DT modular storage subsystem (with fully-redundant power)

Software Components

This section describes the software components necessary to configure and manage a DT storage subsystem. For installation instructions, see Chapter 4, "Configuring a Standard Data Replication Manager Solution."

Array Controller Software

HSG80 Array Controller Software (ACS) is the software component of the HSG80 Array Controller subsystem. ACS software executes on the HSG80 controller and processes I/O requests from the host, performing the device-level operations required to satisfy the requests. The "P" version of the code, for example ACS Version 8.7P, supports DRM.

Secure Path

HP StorageWorks Secure Path is an additional server-based software that enhances the StorageWorks RAID dual-ported storage subsystem by providing automatic error recovery from server-to-storage subsystem connection failures. Secure Path allows you to add redundant Fibre Channel paths between hosts and a RAID storage subsystem, improving overall data availability. If any component in the path between the host and storage subsystem fails, Secure Path immediately redirects all pending and subsequent I/O requests from the failed path to the alternate path, preventing an adapter, cable, or controller failure from disrupting data access.

Secure Path is required for operating systems (such as HP-UX, IBM AIX, Microsoft Windows NT, Microsoft Windows 2000, Novell NetWare, and Sun Solaris) that do not have native multipath support. HP Tru64 UNIX and HP OpenVMS do have native multipath support and do not require Secure Path. Secure Path is a separate product from DRM and must be ordered in addition to ACS Version 8.7P. For more information on Secure Path, refer to the Secure Path documentation for your operating system.

Control and Monitoring Tools

You can use either of the following tools to create LUNs and remote copy sets on the HSG80 controller, and to monitor the status of the HSG80 controllers:

- StorageWorks Command Console (SWCC)
- Terminal emulation to the HSG80 console port

Only one of these tools may be used at any given time for creation and monitoring tasks. See the section titled "Restrictions," on page 31.

StorageWorks Command Console (Optional)

SWCC provides local and remote management of controllers and their attached storage devices. SWCC consists of two major components: the SWCC client and the SWCC agent. SWCC can be used to configure and manage the DT storage subsystem.

The SWCC client is a companion to the agent; it is a graphical user interface (GUI) that runs on a local host and displays the logical and physical layout and status of a selected subsystem in graphical form.

The SWCC agent is a host-resident program that is an interface between the client and the host's storage subsystem that allows the two to communicate over a network.

For a full description of SWCC and how it operates, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide*.

Restrictions

The HSG80 controller does not distinguish between commands issued from in-band command tools (SWCC and Command Scripter) and commands issued out-of-band through the serial port. Serial port commands should only be performed when the customer has restricted commanding from other sources.

Remote Copy Set Features

2

This chapter discusses Data Replication Manager (DRM) concepts you need to know to configure a DRM solution. These concepts primarily describe how to use remote copy sets and association sets.

This chapter discusses the following topics:

- Remote Copy, page 34
  - Remote Copy Sets, page 34
  - Nonremote Copy Sets, page 34
  - Operation Modes, page 34
  - ADD REMOTE_COPY_SETS Command, page 35
- Association Sets, page 37
  - Association Set Characteristics, page 37
  - ADD ASSOCIATIONS Command, page 39
  - Write History Logging, page 39
  - Switches, page 41
  - Failover, page 42
  - Failback, page 43

Remote Copy

DRM uses the peer-to-peer remote copy function of the HSG80 controller to achieve data replication. The HSG80 dual-controllers at the initiator site are connected to their partner HSG80 controllers at the target site. Remote copy sets are mirrors of each other and are created from units at the initiator and target sites. As data is written to a unit at the initiator site, it is mirrored to its remote copy set partner unit at the target site.

The remote copy feature is intended not only for disaster recovery but also to replicate data from one storage subsystem or physical site to another subsystem or site. It also provides a method to perform a backup at either the local or remote site.

With remote copy, user applications continue to run while data movement goes on in the background over a separate interconnect. Data warehousing, continuous computing, and enterprise applications all require remote copy capabilities. The remote copy feature is the major component in the DRM solution.

Remote Copy Sets

A remote copy set is a bound set of two units—one at the initiator site and the other at the target site—for long-distance mirroring. The term *unit* is defined as a single disk, storageset, mirrorset, or RAIDset. The local controller is designated the *initiator*. The initiator acts as the director of the replication process. The corresponding remote controller is designated the *target*. The target receives I/O requests from the initiator to replicate the data at its location.

Remote copy sets are created only at the initiator site. There can be up to 12 remote copy sets per controller.

Nonremote Copy Sets

Nonremote copy sets can exist on the same subsystem at the initiator or the target site, or both, and are generally used for local storage at each site. Clones and snapshots of existing remote copy sets are nonremote copy sets and can be created for activities like testing and backup. Because the nonremote copy sets are unique to the specific controller pair, data is not site disaster tolerant, but can use the various RAIDset types for failure tolerance.

Operation Modes

There are two possible remote copy operation modes: *synchronous* and *asynchronous*. Figure 10 shows the timeline differences between the two.

Synchronous Operation Mode

In synchronous operation mode, data is simultaneously written to the cache of the initiator subsystem and the cache of the target subsystems. The I/O completion status is not sent to the host until all members of the remote copy set are updated. Synchronous operation ensures the highest possible level of data consistency, which makes this process especially appropriate for business applications that require a high level of currency. The default setting is synchronous.

Asynchronous Operation Mode

In asynchronous operation mode, the write operation is reported to the host as complete *before* the data is written to the remote unit of the remote copy set. Asynchronous mode can provide improved response time, but the data on all members of the remote copy set cannot be assumed to be the same at all times.

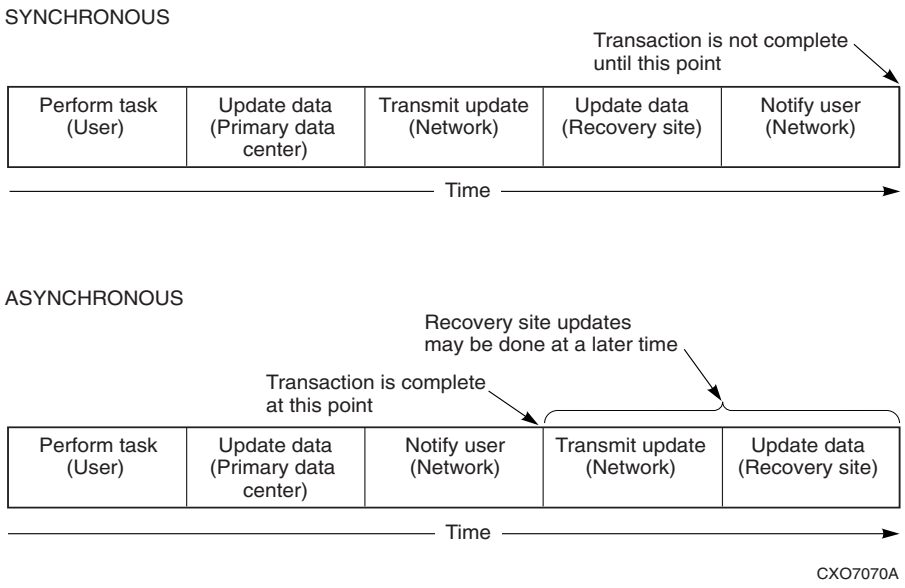


Figure 10: Remote copy set operation modes

Operation Mode Considerations

Consider the following characteristics when designing your DRM configuration:

- Synchronous replication is appropriate when exact consistency is critical to the business application. The application or application recovery depends upon data being written to both local and remote sites.
- The greater the Outstanding I/O setting, the more data can be lost when a disaster occurs at the initiator site. There is no loss of data in synchronous mode.
- Synchronous operation may deliver best response time for heavy host-write operations. In most cases, even though synchronous operation must wait for data to be sent to the target and the target to respond with acknowledgement, it is faster than asynchronous operation due to overhead in the controller when processing asynchronous commands.
- Asynchronous operation improves response time for some workloads.

ADD REMOTE_COPY_SETS Command

The `ADD REMOTE_COPY_SETS` *`RemoteCopySetName InitiatorUnitName RemoteNodeName\TargetUnitName`* command creates a remote copy set and starts a normalization copy to the target unit. During normalization, the controllers copy all data from the initiator unit to the target unit.

Outstanding_IO Settings

The OUTSTANDING_IO setting allows you to control the number of outstanding initiator-to-target writes for a remote copy set. It does not refer to the write queue depth between the host and the controller. This setting can be applied to both synchronous and asynchronous remote copy sets. However, this setting causes different behavior, depending on the remote copy set operation mode.

The default setting is 20 for each remote copy set. There is a shared maximum of 240 available to all remote copy sets on a controller.

Synchronous

For the synchronous operation mode, the OUTSTANDING_IO setting refers to the number of initiator-to-target writes that can be outstanding at any one time. If OUTSTANDING_IO is set to 1 and the host issues four writes to a remote copy set, then only one write is in progress between the initiator and target at a time. The other three writes are queued in the initiator controller. As each write completes at the target, another write is issued from the initiator controller write queue.

Asynchronous

For the asynchronous operation mode, the `OUTSTANDING_IO` setting applies to the number of noncommitted host writes that can be outstanding at one time between the initiator and target. Noncommitted means the write completion status has been returned to the initiator host, but the write has not been completed at the target.

Suppose, for example, that the outstanding I/O is set to 5 and that the host issues a request, waits for completion from the controller, then immediately issues another request. In asynchronous mode, each request issued by the host is completed by the controller very quickly. As a result, the host issues five requests before the remote site has completed the first request. If the host then issues another (sixth) request, it exceeds the value of the outstanding I/O.

When you exceed the outstanding I/O value, the system switches to synchronous mode. As soon as an in-process I/O completes, another is started that attempts to empty the queue and return to true asynchronous operation.

Outstanding Write Operations

Keep in mind that there is a controller-wide limit of 240 outstanding write operations, even if the total number of writes is greater than 240. For example, you might have 12 synchronous remote copy sets, each with a value of 100. The maximum outstanding writes are 240, and not 1200. When 240 outstanding writes are reached, any new writes to the controller are queued on the host.

High Outstanding I/O Values

Use caution when choosing an `OUTSTANDING_IO` setting, because writes to the targets are handled on a FIFO (first in, first out) basis. As a result, remote copy sets with higher `OUTSTANDING_IO` values could potentially starve other remote copy sets if the write rates become very high.

Low Outstanding I/O Values

On the other hand, choosing a lower setting may starve a very active remote copy set. In the case of asynchronous remote copy sets, a lower `OUTSTANDING_IO` value may be appropriate. This lower value limits the number of outstanding noncommitted writes in the event of an initiator site disaster.

Suspend and Resume Switches

The `SUSPEND` switch suspends the update to the remote copy set target and starts the write history logging of write commands and data from the unit.

Note: This switch is valid only in normal error mode with write history logging enabled (not failsafe).

The RESUME switch initiates the mini-merge restore of the specified remote target unit. This switch enables the initiator to read the log unit and send the write commands, in order, to the target, which brings the target into congruency with the initiator. For more information on mini-merge, see "Write History Logging" on page 39.

Note: The `SET AssociationSetName NOLOG UNIT` command terminates any suspended targets that are currently active and marks them for full copy.

Error Mode Switch

The following command sets the error mode condition:

`SET RemoteCopySetName ERROR_MODE=FAILSAFE` or

`SET RemoteCopySetName ERROR_MODE=NORMAL`

The failsafe error mode causes a remote copy set to become failsafe locked if the target becomes inaccessible or the initiator unit fails. When failsafe is locked, the remote copy set is inaccessible.

If a dual link failure occurs, the target is not removed but is marked invalid. When the target is accessible again, a full copy operation is started. When the copy operation is completed, the failsafe locked condition is cleared.

If the error mode switch is set to `NORMAL`, write operations are allowed to continue even when a dual link or disk error is present. `NORMAL` is the default setting.

Note: You cannot enable the failsafe switch with write history logging enabled.

Association Sets

An association set is a group of remote copy sets that share common attributes. Members of an association set can be configured to transition to the same state at the same time. For example, if one association set member assumes the failsafe locked condition, all other members of the same association set assume the failsafe locked condition as well.

An association set may also be used to simply share a write history log between a group of remote copy set members that require efficient use of the log space.

Association Set Characteristics

Things to remember about association sets include:

- Association sets can have up to 12 remote copy sets as members.
- Association sets can share a write history log, if enabled.
- Synchronous or asynchronous operation mode and members may be set differently.
- If `ORDER_ALL` is set, *in order* execution of commands across the remote copy sets in the association set is required.

- If FAIL_ALL is set, and if one member assumes the failsafe locked condition, then all members of the association set assume the failsafe locked condition.
- Association sets reside on the initiator dual controller, as illustrated in Figure 11.

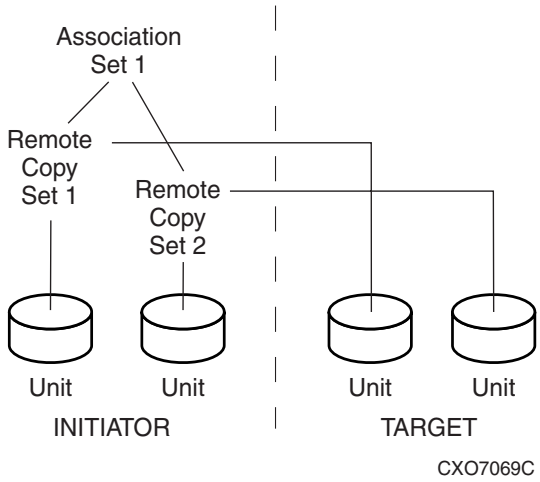


Figure 11: Location of association sets on the initiator dual controller

FAIL_ALL Switch

Because all copy sets within an association set are moved as a unit during failover and failback, all remote copy sets within an association set must be owned by the same server.

If the FAIL_ALL switch is enabled and one member of the association set assumes the failsafe locked condition, all members of the association set assume the failsafe locked condition. The failsafe locked condition prevents further host access.

Note: This applies only to remote copy sets with failsafe error mode enabled. Failsafe error mode is enabled through the ERROR_MODE switch of the SET *RemoteCopySets* command.

When NOFAIL_ALL is specified, the members of the association set react independently to failsafe locked conditions. One member of the association set becoming failsafe locked has no effect on the other members of the association set. NOFAIL_ALL is the default setting.

The NOFAIL_ALL switch has no effect if all members of the association set have failsafe locked error mode disabled (normal error mode) or if there is only one remote copy set in the association.

All members of an association set must be on the same controller, to enforce cache coherency. When members are added to an association set, they are moved to reside on the same controller; they fail over together.

Association set members can be either synchronous or asynchronous. This allows for grouping only those members that use the same write history log unit.

ADD ASSOCIATIONS Command

When you issue the `ADD ASSOCIATIONS AssociationSetName RemoteCopySetName` command, it adds an association set with one member to the controller pair's configuration. Use this command on the node on which the initiator resides. Issue the `SET AssociationSetName ADD = RemoteCopySetName` command to add additional members.

Upon site failover, you must re-create the association sets and log units (see "Write History Log Unit Switches" on page 41) at the target (failover) site, using the attributes that were set at the initiator site.

Write History Logging

Write history logging means using a log unit to record a history of write commands and data from the host. The write history log serves two purposes: to update the target via a mini-merge when the ISL is temporarily broken and to update the initiator as part of the fast failback procedure. In either case, a full copy is not required.

Mini-Merge: When the target becomes accessible again after a failure, a full copy is not necessary. Only those host writes that were performed while the links were down are reissued. This is referred to as a *mini-merge*.

Fast-Failback: During a planned failover, if write history logging has been enabled at the target site, then when the failback is performed, the initiator site is synchronized through a process called *fast-failback*. The writes are logged to the target site write history log. Then, during a fast-failback, the initiator site is updated from the write history log.

If the target becomes inaccessible (because of a dual-target or dual-controller failure), the writes that would have gone to the target are logged to the association set's assigned write history log unit. An inaccessible target in this context refers to both links or target controllers going down.

Remote copy sets are marked for a full copy if they were actively performing write history logging or mini-merging at the time of the controller failure. If a full copy was in progress at the time of the disconnect, write history logging is not initiated and the full copy is restarted when the target is accessible again.

Following a planned failover, if write history logging was enabled at the target site, the initiator site is synchronized during the failback using fast-failback. In this scenario, writes destined for the initiator during the failover period are logged to the association set's write history log unit. This means that only those writes issued since the failover occurred are reissued; a full copy is not necessary.

Write History Log Units

Write history log units are assigned to an association set. Association sets are used by a host to keep multiple units consistent with each other. The write history log unit must always fail over (between dual-redundant controllers) with the remote copy sets assigned to the same association set. *All members of the association set must reside on the same controller* and must fail over both together and automatically. Upon site failover, the user must create a new write history log unit at the target site.

Write History Log Unit Restrictions

Things to remember about write history log units include:

- Up to 12 write history log units can be assigned (12 possible remote copy sets).
- There can be only one write history log unit assigned to an association set.
  - — No new remote copy sets can be added to an association set while write history logging is active.
  - — No new target can be added to a remote copy set that is part of an association set while write history logging is active.
- The write history log unit must be a mirrorset or a striped mirrorset.
- Host access must be disabled to create a write history log unit.
- Write-back caching must be disabled to create a write history log unit.
- Other unit settings must be the default settings to create a write history log unit.
- The write history log unit must reside at the current initiator site.
- Upon site failover, the write history log unit and association set must be reconfigured.
- The write history log unit cannot be a partitioned unit.
- The write history log unit must be a fixed size.

Reaching the End of a Write History Log Unit

Upon reaching the end of the write history log unit:

- The write history log unit is not wrapped and processing does not start over at the beginning. The write history log unit only resets to the beginning when it is empty.
- All active targets engaged in logging or mini-merging will require a full copy when the link is restored or when the `RESUME` command is issued.
- A full copy will occur when the target members are not removed from the remote copy sets.
- You can display a write history log unit utilization with `SHOW REMOTE` and `VTDPY DISPLAY REMOTE` commands.

The time required to reach the end of a write history log unit depends on several factors:

- Size of the write history log unit
- How long the link is down
- How long a target backup takes
- Host write workload
- Number of remote copy sets actively logging to the same unit

Write History Log Unit Performance Considerations

When the write history log unit is merging the captured write operations back to the target, the host makes all I/O resources available to the write history log unit. This means that you can expect at least a 90 percent reduction of host I/O capability for other operations. You must then consider whether the host can afford to perform the merge during normal high-activity hours, or whether the merge should take place during other nonactive times, such as late evening.

A factor in this consideration is what other type of processing the host will be doing during the merge. If the host cannot afford such a drastic reduction in capability, you may wish to consider performing a full copy instead. During a full copy, the host will experience a less drastic I/O performance loss of approximately 50%.

The write history log unit function is primarily intended for, and is most efficient with, short duration outages. If a long duration outage is planned, the full copy option may be the best solution.

Write History Log Unit Size Considerations

Choose the size of the write history log unit carefully. When the end of the write history log unit is encountered, a full copy is initiated when the link is restored. You may wish to select a write history log unit size that will accommodate a maximum outage of 8 hours duration, with the merge occurring during the nonpeak hours that same day.

Display the write history log status by issuing the following CLI command:

```
SHOW REMOTE_COPY FULL
```

Switches

This section discusses the `WRITE HISTORY LOG`, `ORDER_ALL`, `SUSPEND`, and `RESUME` switches.

Write History Log Unit Switches

The `LOG_UNIT` switch of the `ADD ASSOCIATIONS` command assigns a single, dedicated write history log unit for an association set. This switch is valid only if all members of the association set are in normal (not failsafe) error mode. Error mode is determined by the `ERROR_MODE` switch of the `SET` *`RemoteCopySet`* command.

Note: When this command is entered, a header is immediately written to the write history log unit, which may make it difficult or impossible to recover any user data previously written on the unit. Take great care when you specify which unit should be the log unit

---

If `NOLOG_UNIT` is specified, the association set's write history log unit is de-assigned. `NOLOG_UNIT` is the default setting.

Note: A full copy occurs if you disable write history logging after logging operations have begun.

ORDER_ALL Switch

When the ORDER_ALL switch of the ADD ASSOCIATIONS command is enabled, the order of all asynchronous write operations across all members of the association set is preserved. No write history log unit is required.

With the ORDER_ALL switch enabled and write history logging enabled, if one member of the association set starts write history logging, all members of the association set start write history logging. This allows the mini-merge to replay the writes in the same order received from the host.

If NOORDER_ALL is enabled, the members of the association set can start and finish write history independently. NOORDER_ALL is the default setting.

SUSPEND

The SUSPEND switch of the SET *remote-copy-set-name* CLI command allows suspension of write operations to the target so that the target can be used for backup. This switch starts the write history log process for the specified target.

This command is issued at the initiator site, even though the backup is occurring at the target site.

RESUME

The RESUME switch of the SET *remote-copy-set-name* CLI command allows resumption of write operations to the target. The SUSPEND command must previously have been entered for this command to be valid.

This command starts the mini-merge process for restoration of the specified remote target unit.

Failover

There are two types of failover:

- Planned failover (due to a planned takedown of one of the systems, to perform maintenance, for example)
- Unplanned failover (due to a failure within the DRM system)

For more detail on failover and failback, refer to the *HP StorageWorks Data Replication Manager HSG80 Version 8.7P Failover/Failback Procedures Guide.*

Planned Failover

A planned failover allows for an orderly shutdown of controllers. The host applications are quiesced and all write operations are permitted to complete before shutting down the controllers, so that no data is lost or jeopardized. A planned failover requires a synchronous operation mode.

Note: To implement a planned failover while in asynchronous operation mode, you must first switch to synchronous operation.

Unplanned Failover

An unplanned failover does not allow for an orderly shutdown of controllers. An unplanned failover is initiated when any of the following occurs:

- The initiator site is lost.
- There is no host access.
- There is no access to both initiator controllers.

Note: If both links are severed and the initiator configuration is functional, the system administrator must determine which site to use as the primary site.

Failback

The failback method (full copy or fast-failback) is determined by the enabling of logging or failsafe switches, the selected operation mode, and whether the failover is planned or unplanned, as specified in Table 4. This table also shows the availability of the association set switches, ORDER_ALL and FAIL_ALL.

For more detail on failover and failback, refer to the *HP StorageWorks Data Replication Manager HSG80 Version 8.7P Failover/Failback Procedures Guide.*

Table 4: Controller Option Settings for DRM

Logging Enabled					Association Sets	
Logging	Error Mode Failsafe	Operation Mode	Failover	Failback	Order All	Fail All
Enabled	Disabled	Synchronous	Planned	Fast-Failback	Settable	Not Applicable for DRM
Enabled	Disabled	Synchronous	Unplanned	Full Copy	Settable	Not Applicable for DRM
Enabled	Disabled	Asynchronous (switch to Synchronous)	Planned	Fast-Failback	Settable	Not Applicable for DRM
Enabled	Disabled	Asynchronous	Unplanned	Full Copy	Settable	Not Applicable for DRM
Note: Logging is recommended for operations that can tolerate temporary loss of currency at the target site.						
Disabled	Enabled	Synchronous	Planned	Full Copy	Not Applicable for DRM	Settable
Disabled	Enabled	Synchronous	Unplanned	Full Copy	Not Applicable for DRM	Settable
Disabled	Enabled	Asynchronous	Planned	Full Copy	Settable	Settable
Disabled	Enabled	Asynchronous	Unplanned	Full Copy	Settable	Settable
Note: Failsafe is recommended for operations that can tolerate application halt during temporary target inaccessibility.						
Logging and Failsafe both Disabled: Not recommended. Not disaster tolerant						
Logging and Failsafe both Enabled: Not permitted. Logging and failsafe may not be enabled simultaneously.						

Getting Started

3

This chapter explains how to get your Data Replication Manager (DRM) solution ready for setup.

Note: It is a good idea to keep a copy of this manual at both the initiator and target sites to ensure a successful and identical setup at both sites. Two copies also eliminate confusion if more than one person is configuring DRM.

This chapter covers the following topics:

- Site, Host, and Solution Preparation, page 46
  - Host Bus Adapter Requirements, page 46
  - Setting Up the B-Series Fibre Channel Switches, page 46
  - Setting Up the Fiber Optic Cables, page 47
  - Changing SCSI Version from SCSI-2 to SCSI-3 on HSG80 Controllers, page 49
- Cascaded Switches, page 52
  - Hopping, page 52
  - Cascaded Switch Configurations, page 53
- Multiple Intersite Links, page 55

Site, Host, and Solution Preparation

Before you start operating your disaster tolerant (DT) subsystem, you must:

- Ensure that you have sufficient space to install and store the subsystems and have adequate power and cooling resources
- If you choose to use more than one rack, understand the proper methods for positioning and joining subsystems
- Have the proper devices installed
- Verify that all of the storage components are in place

Host Bus Adapter Requirements

To run your DRM solution, you should have two host bus adapters (HBAs) installed on your host system. For detailed information on this hardware, refer to the HBA's user guide that came with your adapter.

At this time, it is important to locate and record the World Wide Names (WWNs) of each HBA. For the HBA at the target site, you can record the WWN in the worksheet provided in Chapter 4, "Configuring a Standard Data Replication Manager Solution." The initiator site HBA WWNs can also be recorded in the worksheet in Figure 19 in Chapter 4. You must have this number handy when you rename the host connections in Chapter 4.

Note: The World Wide Name can be found on the bottom of the HBA board. Look for a small bar code label with an IEEE (Institute of Electrical and Electronics Engineers) precursor. A WWN example is 1000-0000-C920-A5BA.

Setting Up the B-Series Fibre Channel Switches

The Fibre Channel switches must be in place before the DRM subsystems can be cabled and configured. You need the following to install your Fibre Channel switches:

- Power cord
- 10Base-T cable with RJ-45 connector (to be connected to an Ethernet hub or switch)
- Fixed IP address and subnet mask (one of each per switch)

The Ethernet cable and IP address are required to monitor and administer the Fibre Channel switch. Configure the Ethernet IP address and the Ethernet IP subnet mask with the front panel buttons of the Fibre Channel switch (16-port switches only).

For B-series (1 Gb) switches, keep the following in mind:

- A single fabric can contain no more that 28 switches.
- No more that 50% of the ports can be connected to intersite links (ISLs).
- Each intersite link (ISL) can support a maximum of from 7 to 11 end devices (hosts, controllers, and so on), depending on the host operating system and load.

For other switch families (C-series and M-series) see the *HP StorageWorks SAN Design Reference Guide* for current fabric limits.

When the Ethernet IP settings are established, perform the following steps:

1. *Ping* the switch using the Ethernet IP address of the switch. If this is successful, you have access to the switch.

2. *Ping* using the name of the switch. This verifies the operation of the name resolution.
3. *Telnet* into the switch (username = admin; password = password [default setting]). Refer to your switch documentation for Telnet session procedures. Make the following adjustments to the switch:
   — Enter `switchName` to configure the switch name. Be sure to designate a name that enables you to easily identify the switch you are trying to access.

     Example: `switchName NewSwitchName`
   — Enter `switchShow` to reveal the status of the switch and some of its ports.
   — Enter `version` to display the firmware levels. For updated version information, go to the DRM Release Notes.
4. Using a Java-capable browser, go to http://<FC switch DNS name> to view a visual representation of the switch. (You need to know the Domain Server Name.) You can double-click this picture for further information.

For procedures related to the other switch families (C-series and M-series), refer to the appropriate vendor documentation.

Setting Up the Fiber Optic Cables

Before you connect the fiber optic cables to your subsystems, it is important to understand the designated names of each component. See Table 5 on page 49 for an overview list of required connections for each site and between the sites.

Note: For instructions on making connections, refer to Chapter 4, "Configuring a Standard Data Replication Manager Solution."

Figure 12 shows how each component is referenced in this document.

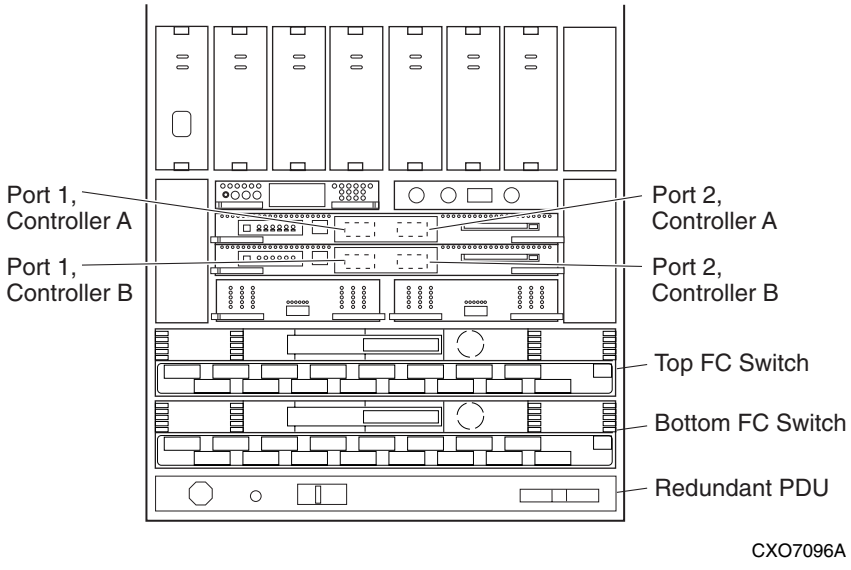


Figure 12: Locations and names of components for connecting fiber optic lines

Before you connect the fiber optic cables, HP recommends that you tag each end of the cables with the following information.

Host-to-Switch Connections

- Host name and rank number or PCI slot number of the HBA
- Switch name and port number on switch

Switch-to-Controller Connections

- Fibre Channel switch name (top or bottom)
- Fibre Channel switch port number (0-15 for a sixteen port switch)
- Site name (initiator or target)
- Controller name
- Controller port number (1 or 2)
- Host port number
- HBA WWN

The DT solution requires two different types of fiber optic cables, depending on where the connections are made. Cabling at each individual site that involves the controller, the switch, and the host is made with 50-micron multimode fiber optic cables. The maximum length that these cables support is 500 meters. When cabling between initiator and target sites that are more than 500 meters apart using GBICs, you must use a 9-micron single-mode fiber optic cable, which can run a distance of up to 100 km, depending on the GBIC and the quality of the cable connection. For additional information refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide.*

Note: The 9-micron single-mode fiber optic cable may also be referenced by some manufacturers as an 8.3-micron cable. To increase the reliability of the cable or to reduce the likelihood of having to re-pull or re-install the cable over a long distance, HP recommends that you use multiple conductor cable.

For a list of the most current software, firmware, patches, drivers, and so on, for each of the supported operating systems in your DRM solution, refer to the DRM Release Notes.

Caution: If the fiber optic cable is not properly connected to the controller, failure may result. Because of the cable's frail nature, it must be regularly maintained or its performance and life span will be affected. Before continuing, make sure that you follow the precautions listed in the *HP StorageWorks HSG80 Array Controller ACS Version 8.7 Maintenance and Service Guide*.

Table 5 provides an example of the connections required at each site and between the sites for the first server and first storage array. Note that additional servers and additional arrays will use other ports. Specific connection information is covered in more detail in Chapter 4, "Configuring a Standard Data Replication Manager Solution."

Caution: Do not make any connections until you are instructed to do so later in this guide.

Table 5: Example of Wiring for First Server and First Storage Array at Each Site

Initiator Site			Target Site		
Host Port 1	→	Top Switch, Port 0	Host Port 1	→	Top Switch, Port 0
Host Port 2	→	Bottom Switch, Port 0	Host Port 2	→	Bottom Switch, Port 0
Controller A, Port 1	→	Top Switch, Port 2	Controller A, Port 1	→	Top Switch, Port 2
Controller A, Port 2	→	Top Switch, Port 4	Controller A, Port 2	→	Top Switch, Port 4
Controller B, Port 1	→	Bottom Switch, Port 2	Controller B, Port 1	→	Bottom Switch, Port 2
Controller B, Port 2	→	Bottom Switch, Port 4	Controller B, Port 2	→	Bottom Switch, Port 4

Between Initiator and Target Site				
Top Switch, Port 6	→	External Fiber Link	←	Top Switch, Port 6
Bottom Switch, Port 6	→	External Fiber Link	←	Bottom switch, Port 6

Note that additional servers and storage arrays will use other ports.

Changing SCSI Version from SCSI-2 to SCSI-3 on HSG80 Controllers

SCSI-3 is the preferred protocol for DRM. If your operating system supports SCSI-3, HP recommends that you change from SCSI-2 to SCSI-3. You can use either the static or rolling upgrade procedure for this change.

Static Upgrade Procedure

This procedure requires that you stop all I/O and unmount all devices to the HSG80 controllers.

1. Verify that your host's operating system supports SCSI-3. You can determine this by referring to the DRM Release Notes.
2. Check for LUN 0 and unused devices on the SCSI-2 HSG80 controllers by issuing the following CLI command:

   ```
   SHOW UNITS
   ```

   You will see a display similar to Example Display 1.

Example Display 1

```
BuildngBTop> SHOW UNITS
  LUN                     Uses             Used by
------------------------------------------------------------
  D1                      DISK10000
  D2                      DISK20000
  D3                      R3
  D4                      R4
  D5                      S5
  D6                      M6
  D11                     DISK30100
  D20                     MIR_DLOG
  D21                     MIR_LOGD
  D199                    DISK30300
  BuildngBTop>
```

In this example there is no D0 and there is an available LUN (D7) to use (note that D7 is missing from the list). Had there been a D0, you would need to delete the D0, then add unit D7. All LUN 0 devices must be changed to an unused LUN.

This step is necessary because the controllers in SCSI-3 mode automatically use LUN 0 for the Command Console LUN.

3. Stop all I/O and unmount all devices to the HSG80 controllers.
4. Verify that the HSG80 controllers are in SCSI-2 mode by issuing the following CLI command:

   ```
   SHOW THIS_CONTROLLER
   ```

   You should see a display similar to that in Example Display 2.

Example Display 2

```
Controller:
HSG80 ZG84906303 Software  ACS 8.7P-0, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-01F0
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
        Configured for MULTIBUS_FAILOVER with ZG84906237
            In dual-redundant configuration
        Device Port SCSI address 7
        Time: 02-APR-2002 14:06:48
        Command Console LUN is disabled
        Host Connection Table is LOCKED
        Smart Error Eject Disabled
       .
       .
       .
```

5. Change to SCSI-3 mode by issuing the following CLI command:

   ```
   SET THIS_CONTROLLER SCSI_VERSION=SCSI-3
   ```

   You should see a display similar to that in Example Display 3.

Example Display 3

```
BuildngATop> set this_controller scsi_version=scsi-3
Warning 4030: Any units that would appear as unit 0 to a host will not be
              available when in SCSI-3 mode
Warning 4020: A restart of both this and the other controller is required
              before all the parameters modified will take effect
%CER--BuildngATop> --01-APR-2002 14:11:00-- Restart of this controller required
%CER--BuildngATop> --01-APR-2002 14:11:01-- Restart of the other controller-
required
Restart of this controller required
Restart of the other controller required
```

6. Issue the following restart CLI commands:

   ```
   RESTART OTHER_CONTROLLER
   RESTART THIS_CONTROLLER
   ```

7. When both controllers are restarted, verify that the HSG80 controllers are in SCSI-3 mode by issuing the following CLI command:

   ```
   SHOW THIS_CONTROLLER
   ```

   You should see a display similar to that in Example Display 4.

Example Display 4

```
Controller:
        HSG80 ZG84906303 Software ACS 8.7P-0, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-01F0
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-3
        Configured for MULTIBUS_FAILOVER with ZG84906237
            In dual-redundant configuration
        Device Port SCSI address 7
        Time: 02-APR-2002 14:24:21
        Command Console LUN is lun 0 (NOIDENTIFIER)
        Host Connection Table is LOCKED
        Smart Error Eject Disabled
       .
       .
       .
```

8. Repeat steps 1 through 7 at the other site's HSG80 controller pair.
9. Enable access to HSG80 devices using the method for your OS type.

Rolling Upgrade Procedure

This procedure allows you to change from SCSI-2 to SCSI-3 without stopping all I/O to the HSG80 controllers. Use this procedure if you cannot be without constant access to your storage. The procedure is the same as for the static upgrade above, except for the following:

1. Do not perform step 3 above to stop I/O and unmount devices.
2. Replace step 6 above with the following step 6:

   6. Issue the following restart CLI command:

      ```
      RESTART OTHER_CONTROLLER
      ```

      LUNs assigned to the OTHER controller will fail over to THIS controller. When the controller has fully rebooted and is back online, issue the following CLI command:

      ```
      RESTART THIS_CONTROLLER
      ```

Cascaded Switches

Cascaded switches provide a DRM configuration variation that lets you:

- Increase the distance between sites (expand the fabric)
- Increase host or controller port connections

A *cascaded switch* is one where the output of one switch is connected to the input of another. The second switch may then be connected to another switch, a host, or a controller.

Hopping

The cascading of switches employs hopping. A *hop* is defined as one or more connections between two Fibre Channel switches. Two switches cascaded are equal to one hop. Server-to-Fibre-Channel switch segments and storage-to-Fibre-Channel switch segments are not counted as hops.

The definitive resource for SAN configuration rules is the *HP StorageWorks SAN Design Reference Guide*, which is available at the following website:

http://h18006.www1.hp.com/products/storageworks/san/documentation.html

The following rules apply to hops in a DRM environment:

- For B-series switches: Maximum of 28 switches in a fabric with no more than 7 hops allowed from the host to either the initiator controller or the target controller.
- For C-series switches: Maximum of 11 switches in a fabric with no more than 3 hops allowed from a host to either the initiator or target controller.
- For M-series switches: Maximum of 24 switches in a fabric with no more than 3 hops allowed from a host to either the initiator or target controller.
- Within a single fabric where switches are interconnected, each Fibre Channel switch must have a unique domain number (Domain_ID.)
- The maximum distance allowed using short wavelength laser GBICs and 50-micron multimode fiber optic cable is 500 meters per cable segment.
- The maximum distance allowed using long wavelength laser GBICs and 9-micron single-mode fiber optic cable is 10 kilometers per cable segment.
- Very Long Distance GBICs can extend ISLs up to 100 kilometers.
- Wavelength Division Multiplexing (WDM) can extend up to 120 kilometers.

- Only one extended long wavelength ISL is allowed per fabric.
- Cascaded switches are not supported in asynchronous transfer mode (ATM) configurations.

Cascaded Switch Configurations

Figure 13 shows a DRM configuration that increases the distance between sites by using cascaded switches and hopping. There are no hops from the initiator host to the initiator controller and three hops from the initiator host to the target controller. There are four Fibre Channel cascaded switches with no hops from the host and three hops to controller pair 2. Hop 1 spans the shortest distance (500 meters), hop 2 spans 10 kilometers, and hop 3 spans the longest distance, 100 kilometers.

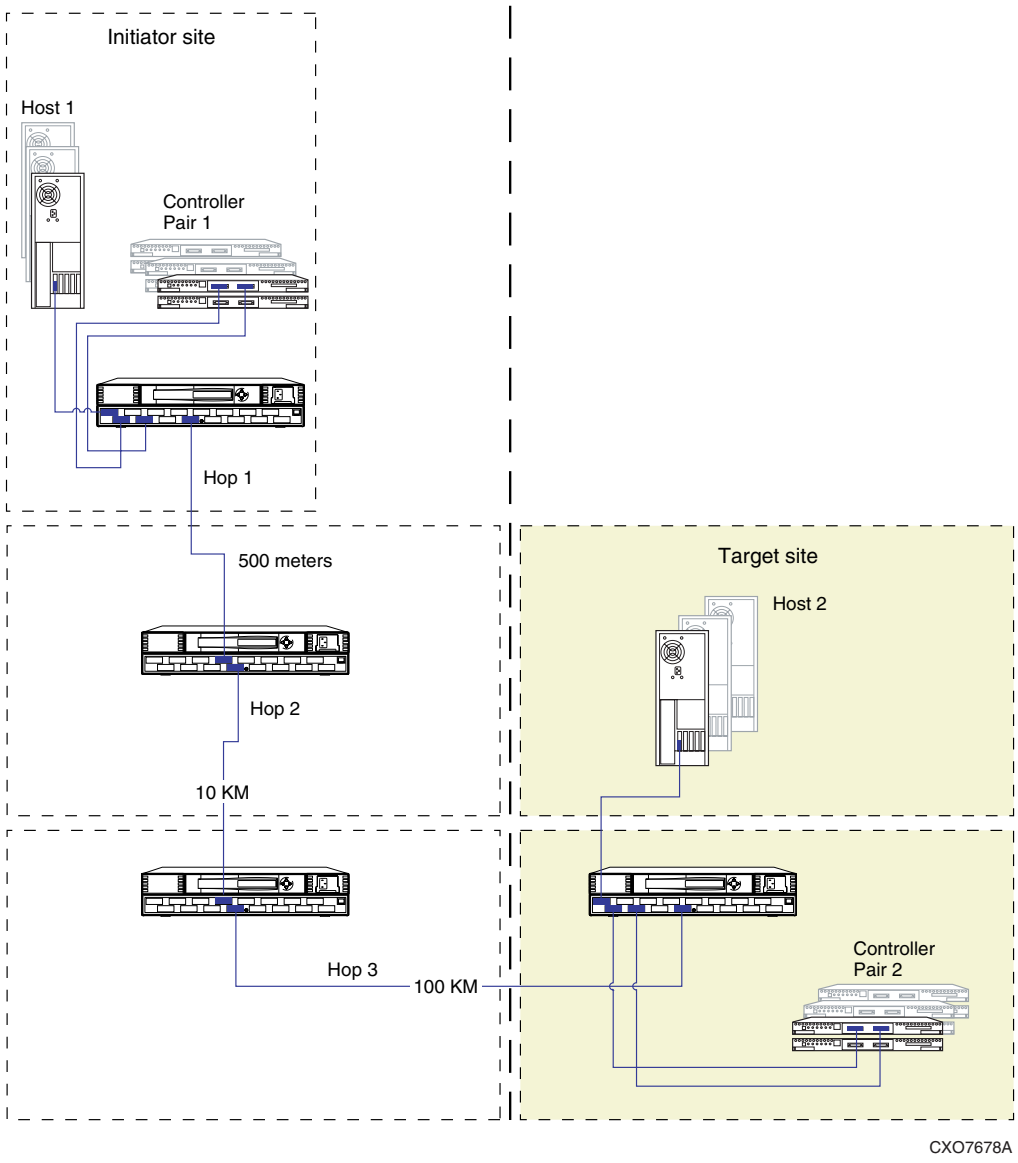


Figure 13: Cascaded switches in a DRM environment

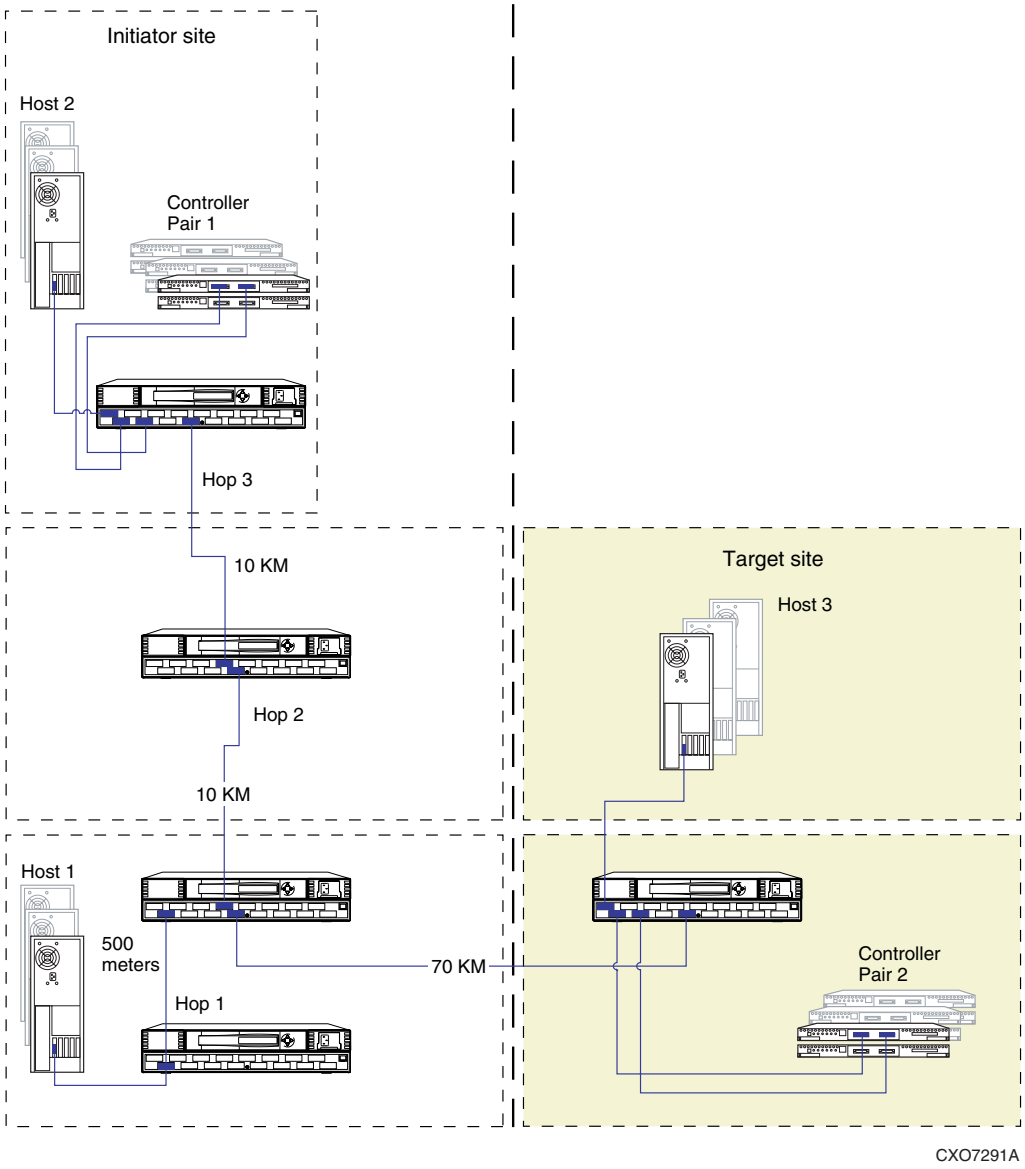


Figure 14: Cascaded switches in DRM environment with three hops between host and controller

Figure 14 shows a DRM configuration that increases the number of host-to-controller port connections using cascaded switches and hopping. The figure features switches cascaded from Host 1 to the initiator controller. There are four Fibre Channel cascaded switches, three hops from Host 1, and three hops to the initiator controller pair 1.

Multiple Intersite Links

Multiple intersite links (ISLs) provide additional bandwidth between local and remote sites. Each ISL is a fiber link between two switches.

The restrictions that apply when using multiple ISLs in a DRM environment are listed below:

- DRM supports a maximum of two ISL connections per fabric.
- The Multiple E-port Connectivity software option is required to access more than one E-port when using multiple ISLs or interswitch links with the SAN Switch 8-EL.
- For a cascaded switch configuration, the SAN switch 8-EL must be placed at the end of the cascade to provide access to the E-port, unless the Multiple E-port Connectivity software option is used.

You can increase bandwidth on the ISL by adding an additional link in parallel between the same two switches, as shown in Figure 15. DRM supports two connections, maximum. The switches are shown as physically connected, although the connections are transparent to the fabric. Functionally, the devices appear to be connected directly together.

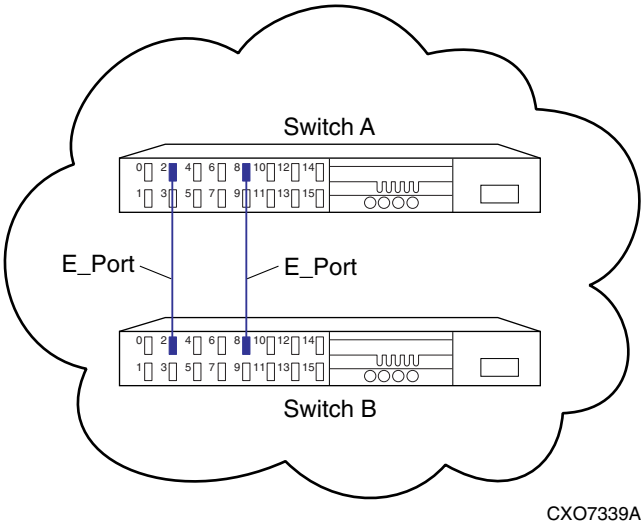


Figure 15: Multiple intersite links

Configuring a Standard Data Replication Manager Solution

4

This chapter provides procedures for configuring your Data Replication Manager (DRM) solution. Because a DRM system spans two sites, you must configure the DRM system at each site.

These procedures take you through the configuration process. You will first set up the target site, then the initiator site. Setup for each site is similar. At each site, you will configure the controllers by defining controller characteristics specific to DRM. You will then define storagesets, units, remote copy sets, and association sets. After the controllers are configured, you will make fiber optic cable connections between the controllers and switches. Finally, you will install the necessary software and drivers on each host.

This chapter covers the following topics:

- Introduction, page 58
- Configuration Overview, page 60
- Configure the Controllers at the Target Site, page 62
- Configure Storage at the Target Site, page 69
- Cable the Target Site, page 71
- Create Switch Zones at the Target Site, page 74
- Configure the Host at the Target Site, page 74
- Configure the Controllers at the Initiator Site, page 100
- Configure Storage at the Initiator Site, page 107
- Cable the Initiator Site, page 109
- Connect the Initiator Site to the External Fiber Link, page 111
- Create Switch Zones, page 112
  - — Create Connections from the Target Site, page 112
- Create Write History Log Units and Association Sets (Optional), page 115
- Configure the Host at the Initiator Site, page 118
- Additional Host Configuration, page 144
- Documenting Your Configuration, page 145

Introduction

The disaster tolerant (DT) configuration that supports DRM requires two HSG80 Array Controller subsystems—one at an initiator site and one at a target site.

Tip: Because of the complexity of the configuration process, it is a good idea to have all DRM documentation available at both sites to eliminate confusion and minimize the risk of error. Follow the steps precisely in the order provided in this document.

Figure 16 shows a basic DRM configuration; it is referenced throughout this chapter.

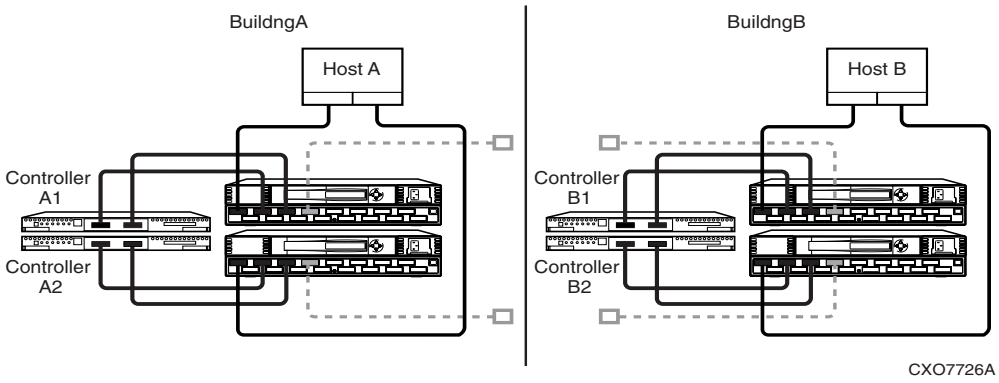


Figure 16: Basic Data Replication Manager configuration

Restrictions

It is important to understand the operating restrictions before configuring your DRM solution. Table 6 lists points to consider before proceeding to the configuration process.

Table 6: Restrictions and Requirements

Restriction or Requirement	Comments
Two HSG80 controller pairs are required.	All controllers must run ACS V8.7P. HSG60 controller pairs are not supported.
Four Fibre Channel switches are required. (The entry-level DRM configurations introduced in Chapter 5 are exceptions to this restriction).	These switches provide two separate fabrics connecting controllers at the initiator and target sites.
HSG80 controllers can be configured for Fibre Channel switched protocol and SCSI-2 or SCSI-3 protocol.	HP OpenVMS host operating systems and adapters must support Fibre Channel switched protocol and SCSI-3 protocol Except OpenVMS, the host operating systems and adapters must support Fibre Channel switched protocol and SCSI-2 or SCSI-3 protocol.
Mirrored write-back cache must be enabled.	Requires 512 MB of cache per controller (256 MB effective capacity when mirrored).

Table 6: Restrictions and Requirements (Continued)

Restriction or Requirement	Comments
Maximum configuration for all platforms except Novell NetWare: 12 equivalent hosts per storage array 6 host bus adapters (HBAs) per host 24 units per host 8 subsystems per site	There must be least two HBAs per server; refer to the OS-dependent restrictions in the *HP StorageWorks SAN Design Reference Guide*.
Maximum configuration for NetWare: 4 HBAs per host	2 HBAs per host minimum.
For IBM AIX, there is a maximum of 32 LUNs per storage array.	LUNs 1 to 32 are available; LUN 0 is the Command Console LUN (CCL).
Maximum of 12 remote copy sets allowed per HSG80 controller pair.	If more than 12 remote copy sets are needed, additional subsystems are required.
Maximum of 2 unit members allowed per remote copy set.	Composed of 1 initiator unit and 1 target unit.
Maximum of 12 nonremote copy set LUNs at initiator and target sites.	
Target unit cannot reside on the same controller pair as its initiator unit.	One controller pair required for initiator; one controller pair required for target.
Controller replication conducted through port 2 on each controller.	Link between initiator and target site is made through port 2. Both port 2 links (top and bottom controllers) must be up when DRM setup is configured.
Maximum of 96 connections.	Effective number of connections is 96 minus the 4 default remote copy connections. More than 96 connections may require use of switch zoning to restrict visible devices.
DILX (disk inline exerciser) cannot be run on units used by remote copy sets.	Run DILX prior to creating the remote copy set configuration. For information on DILX, refer to the *HP StorageWorks HSG80 Array Controller ACS Version 8.7 CLI Reference Guide.*
The LUN/unit at the initiator and target sites must be identical.	Keep the unit number, RAID level, disk geometry used, and other parameters the same to eliminate confusion and risk of error.
Controller-based partitions are not supported within remote copy sets.	Host software may be capable of partitioning units.
Units at the initiator and target sites cannot be transportable units.	Units cannot be moved to noncontroller configurations without potential data loss.
FRUTIL cannot be used on remote site while I/O is in progress to target site.	For information on *FRUTIL*, see the *HP StorageWorks HSG80 Array Controller ACS Version 8.7 CLI Reference Guide.*
Write history log units must: ■ Reside at the initiator site ■ Not be moved to the target site ■ Not be a partitioned unit ■ Have mirrored write-back cache disabled ■ Have all access disabled ■ Be re-created at target site after failover ■ Be a mirrorset	Can be a 1-member mirrorset.

Table 6: Restrictions and Requirements (Continued)

Restriction or Requirement	Comments
HP storage arrays running ACS 8.5F, 8.5S, 8.5P, 8.6F, and 8.6S may co-exist on the same SAN with a DRM configuration using ACS 8.7P.	
For OpenVMS, the LP7000 and LP8000 HBAs may coexist on the same DRM storage area network. However, they may not share the same server. IBM AIX supports only Cambex HBAs.	
Zoning is required when there is more than one Tru64 TruCluster. See Chapter 6, "Configuring the Optional Advanced DRM Solutions," and the *HP StorageWorks SAN Design Reference Guide* for details on switch zoning.	
Boot disks on the HSG80 for OpenVMS must be nonremote copy set devices.	
DRM does not support the bootless failover of the system disk by any of the supported operating systems.	

For a list of additional software support required for each operating system in your DRM solution, refer to the DRM Release Notes.

Configuration Overview

Both the initiator and target sites need a command line interface (CLI) to the controller. You can connect the serial maintenance port of both the initiator and target site controllers to a terminal supporting multiple serial connections, or to multiple terminals, from which to issue CLI commands. You can also start a terminal emulator session from the platform of your choice (for example, HyperTerminal in Windows). The default settings are 9600 baud, 8 bits, no parity, 1 stop bit.

Terminal emulator sessions require either a direct serial connect from the server to the controller, or an intermediate terminal server. If you use a terminal server, the connection from the server running the emulator to the terminal server will be over a standard network, not a serial connection.

Configuration Procedures Outline

Target Site Outline

- Configure the Controllers at the Target Site
- Configure Storage at the Target Site
  - Devices and Storagesets
  - Create Storage Units
- Cable the Target Site
  - Connect Fiber Optic Cables Between Controllers and Fibre Channel Switches
  - Connect the Target Site to the External Fiber Link

- Create Switch Zones at the Target Site
- Configure the Host at the Target Site
  - HP OpenVMS
  - HP Tru64 UNIX
  - HP-UX
  - IBM AIX
  - Microsoft Windows NT and Windows 2000
  - Novell NetWare
  - Sun Solaris

Each of these steps is discussed in detail in the sections beginning on page 62.

Initiator Site Outline

- Configure the Controllers at the Initiator Site
- Configure Storage at the Initiator Site
  - Devices and Storagesets
  - Create Storage Units
- Cable the Initiator Site
  - Connect Fiber Optic Cables Between Controllers and Fibre Channel Switches
- Connect the Initiator Site to the External Fiber Link
- Create Switch Zones
- Create Remote Copy Sets
  - Prepare the Initiator Site
  - Create Connections from the Target Site
  - Create Remote Copy Sets from the Initiator Site
  - Set Failsafe at the Initiator Site (Optional)
- Create Write History Log Units and Association Sets (Optional)
  - Create a Write History Log Unit
  - Create Association Sets and Assign a Write History Log Unit
- Configure the Host at the Initiator Site
  - HP OpenVMS
  - HP Tru64 UNIX
  - HP-UX
  - IBM AIX
  - Microsoft Windows NT and Windows 2000
  - Novell NetWare
  - Sun Solaris

Each of these steps is discussed in detail in the sections beginning on page 100.

Configure the Controllers at the Target Site

Note: Target site procedure steps are marked with a target symbol, ⊙. Initiator site procedures are marked with an initiator symbol, ⊳.

Before configuring the controllers at the target site, follow these preparatory steps:

⊙ 1. Identify the World Wide Name (WWN) on the HBAs in each host.

⊙ 2. Establish the names to assign to the target and initiator sites. Use a naming convention that is meaningful, like building or city names; for example, name the initiator site *BuildngA* and target site *BuildngB*.

Note: These names may be a maximum of nine characters. They may consist of alphanumeric characters and special characters, except for the comma (,) and backslash (\ ).

If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

To get your DT system up and running, you must set up and configure the controllers. These tasks are outlined in the following procedure:

⊙ 1. Ensure that all enclosures, Fibre Channel switches, and power distribution units (PDUs) are powered off.

⊙ 2. Plug all rack PDU power cords into the main power receptacles.

⊙ 3. Make sure that you have a serial connection ready to the maintenance port of each controller. Refer to the *HP StorageWorks HSG80 Array Controller ACS V8.7 Maintenance and Service Guide* for instructions.

⊙ 4. Power on all PDUs.

⊙ 5. Ensure that the Fibre Channel switches are powered on, but not cabled.

Note: When the enclosures are turned on, the controllers start only if the PCMCIA cards are already installed. If there are no cards in the controller slots, insert them now and press the **Reset** button. Refer to the *HP StorageWorks HSG80 Array Controller ACS V8.7 Maintenance and Service Guide* for complete instructions on properly seating the controller firmware cards.

⊙ 6. Turn on the enclosures.

⊙ 7. Establish a CLI connection to the bottom controller. Refer to the *HP StorageWorks HSG80 Array Controller ACS V8.7 Maintenance and Service Guide* for instructions.

⊙ 8. Verify that the bottom controller is on and functional by looking for the CLI prompt on the maintenance port.

9. Establish a CLI connection to the top controller.
10. Verify that the top controller is on and functional by looking for the CLI prompt on the maintenance port.

Note: Unless otherwise noted, all operations may be conducted from the top controller (controller B1).

---

11. To verify that the controllers are properly set up, issue the CLI command:

    ```
    SHOW THIS_CONTROLLER
    ```

    You should see a display similar to that in Example Display 1.

Example Display 1

```
Controller:
   HSG80 ZG8nnnnnnn Software V87P, Hardware  E03
   NODE_ID          = nnnn-nnnn-nnnn-nnnn
   ALLOCATION_CLASS = 0
   SCSI_VERSION     = SCSI-2
   Not configured for dual-redundancy
   Controller misconfigured -- other controller present
   Device Port SCSI address 7
   Time: NOT SET
   Command Console LUN is disabled
   Host connection table is NOT locked
   Smart error eject disabled
Host PORT_1:
   Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
   PORT_1_TOPOLOGY  = OFFLINE (offline)
Host PORT_2:
   Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
   PORT_2_TOPOLOGY  = OFFLINE (offline)
   NOREMOTE_COPY
Cache:
   512 megabyte write cache, version 0012
   Cache is GOOD
   No unflushed data in cache
   CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
Mirrored Cache:
   Not enabled
Battery:
   FULLY CHARGED
   Expires: . . . . . .
   NOCACHE_UPS
```

12. Verify that the subsystem WWN (also called the *NODE_ID*) has been assigned to the controller. If zeros are displayed, the name is not set.
    - If the name is set, go to step 15.
    - If the WWN has not been assigned to the controller, you must obtain the name and set it before proceeding.

Note: The subsystem's WWN and checksum are located on a sticker on top of the frame that houses the controllers, EMU, PVA, and cache modules. The checksum is required to verify that the WWN is valid. If there is no label on the frame, contact your HP customer service representative for assistance. Refer to Chapter 7 for more information on WWNs. Each subsystem's WWN begins with 5000 and ends with a zero; for example, 5000-1FE1-FF0C-EE00. The controller port IDs are derived from the WWN.

Caution: Never set two subsystems to the same WWN; data corruption will occur.

13. After the WWN has been located (in step 12), assign it to the controller:

    `SET THIS_CONTROLLER NODE_ID=`*`node_ID checksum`*

    You should see a display similar to that in Example Display 2.

Example Display 2

```
Warning 4000: A restart of this controller is required before all the
   parameters modified will take effect
%CER--HSG80> --09-FEB-1999 10:07:54-- Restart of this controller required
Restart of this controller required
```

Note: Do not restart the controller until the procedure instructs you to do so.

14. Issue a `SHOW THIS_CONTROLLER` command to verify that the WWN has been set.

    You should see a display similar to that in Example Display 3.

Example Display 3

```
Controller:
            HSG80 ZG8nnnnnnn Software V87P, Hardware  E03
            NODE_ID          = YYYY-YYYY-YYYY-YYYY
            ALLOCATION_CLASS = 0
            SCSI_VERSION     = SCSI-2
            Not configured for dual-redundancy
                Controller misconfigured -- other controller present
            Device Port SCSI address 7
            Time: NOT SET
            Command Console LUN is lun 0 (NOIDENTIFIER)
```

15. Configure the controllers for multiple-bus failover mode:

    ```
    SET MULTIBUS_FAILOVER COPY = THIS_CONTROLLER
    ```

    This command automatically restarts the OTHER controller.

    You should see %LFL and %EVL prompts. Refer to the *HP StorageWorks HSG80 Array Controller ACS V8.7 Maintenance and Service Guide* for more information on these reports.

16. To ensure that the setting from step 15 has been applied, issue the command:

    ```
    SHOW OTHER_CONTROLLER FULL
    ```

    Check the display to verify that the controllers have been configured to support multiple-bus failover mode. You should see a display similar to that in Example Display 4.

Example Display 4

```
Controller:
   HSG80 ZG8nnnnnnn Software V87P, Hardware  E03
   NODE_ID          = nnnn-nnnn-nnnn-nnnn
   ALLOCATION_CLASS = 0
   SCSI_VERSION     = SCSI-2
   Configured for MULTIBUS_FAILOVER with ZG8nnnnnnn
   In dual-redundant configuration
   Device Port SCSI address 7
   Time: NOT SET
   Command Console LUN is lun 0 (NOIDENTIFIER)
  .
  .
  .
```

Note: These settings are applied automatically to the bottom controller (controller B2). It is not necessary to repeat these steps on controller B2.

17. You must select the SCSI mode for the subsystem. Some operating systems support only one SCSI mode. For more information, refer to the DRM Release Notes.

    a. To set SCSI-3 mode:

    ```
    SET THIS SCSI = SCSI-3
    ```

Note: For OpenVMS, set allocation class and identifier:

```
SET THIS ALLOCATION_CLASS = 1
SET THIS_CONTROLLER IDENTIFIER = 99
```

Setting this switch causes the host to load the SYS$DRIVER, which provides the GG devices. The value range is 1 - 99.

D0 (D-zero) can no longer be used as a device LUN in SCSI-3 mode.

b. To set SCSI-2 mode:

```
SET THIS SCSI = SCSI-2
```

18. Change your controller prompts to identify which controller you are working on:

```
SET THIS_CONTROLLER PROMPT="TargetControllerNameTop> "
SET OTHER_CONTROLLER PROMPT="TargetControllerNameBottom> "
```

Example: `set this_controller prompt="BuildngBTop> "`

Example: `set other_controller prompt="BuildngBBottom> "`

Note: This step takes effect immediately.

19. Determine whether mirrored write-back cache is enabled:

```
SHOW THIS_CONTROLLER
```

You should see a display similar to that in Example Display 5.

Example Display 5

```
.
.
.
Mirrored Cache:
Not enabled
.
.
.
```

If mirrored write-back cache is not enabled, issue the following CLI command:

```
SET THIS_CONTROLLER MIRRORED_CACHE
```

The controllers restart after mirrored write-back cache has been set. You should see `%LFL` and `%EVL` displays.

Note: It may take up to five minutes after restart for diagnostics to complete on the cache. The controller rejects this command until the cache check is complete. If the command is rejected, do not restart the controllers. Wait a few minutes and then try again.

20. Confirm that mirrored write-back cache is enabled:

```
SHOW THIS_CONTROLLER
```

If the command is accepted, you should see a display similar to that in Example Display 6.

Example Display 6

```
.
.
.
Mirrored Cache:
   256 megabyte write cache, version 0012
   Cache is GOOD
   No unflushed data in cache
.
.
.
```

If the command is rejected, do not restart the controllers. Wait a few minutes and then try again.

Note: It is not necessary to repeat this step on controller B.

---

21. Set the fabric topology for each port on both controllers by issuing the following CLI commands:

Note: You are prompted to restart the controllers after each command, but you do not need to restart the controllers until all topologies have been set.

```
SET THIS_CONTROLLER PORT_1_TOPOLOGY=FABRIC
SET THIS_CONTROLLER PORT_2_TOPOLOGY=FABRIC
SET OTHER_CONTROLLER PORT_1_TOPOLOGY=FABRIC
SET OTHER_CONTROLLER PORT_2_TOPOLOGY=FABRIC
```

22. Issue the CLI command:

```
SET LOG NOLOG
```

Note: You can ignore the error message `ERROR B020:No Logdisk is Configured` if it appears.

---

23. Restart the controllers by issuing the following CLI commands in the order shown:

```
RESTART OTHER_CONTROLLER
RESTART THIS_CONTROLLER
```

Note: There may be a brief delay before control is returned.

---

24. After the controllers have restarted, verify that the topology is set correctly:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You should see a display similar to that in Example Display 7.

Example Display 7

```
.
.
.
Host PORT_1:
   Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
     . . . . . .PORT_1_TOPOLOGY  = FABRIC (connection down)
   Address . . . . . .=nnnnnn
Host PORT_2:
   Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
     . . . . . .PORT_2_TOPOLOGY  = FABRIC (connection down)
   Address . . . . . .=nnnnnn
   NOREMOTE_COPY
.
.
.
```

25. Enable remote copy functionality:

    `SET THIS_CONTROLLER REMOTE_COPY=`*`TargetControllerName`*

    Example: `set this_controller remote_copy=BuildngB`

Note: Be sure to specify a meaningful target controller name, such as a name that reflects the target node's location. The name can be up to eight characters and must be unique to all of your controllers. Do not use *init, initial, rem,* or *remote*; they are reserved keywords.

After you have issued this CLI command, you see a series of `%LFL` and `%EVL` displays; the controllers automatically restart.

26. Verify that these settings are in place:

    `SHOW THIS_CONTROLLER`

    You should see a display similar to that in Example Display 8.

Example Display 8

```
.
.
.
Host PORT_2:
   Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
     . . . . . PORT_2_TOPOLOGY  = FABRIC (up)
   REMOTE_COPY = BuildngB
.
.
.
```

Configure Storage at the Target Site

Before you can configure the storage for DRM, you must add disks, create the storagesets, and create units.

Devices and Storagesets

Before you can configure the storage for remote replication, you must add disks, create storagesets, and create units. Follow the instructions in the HP StorageWorks HSG80 ACS Solution Software Version 8.7 Installation and Configuration Guide for your operating system, but note the restrictions listed in Table 6 of this document.

Note: D0 (D-zero) can no longer be used as a device LUN in SCSI-3 mode.

The target site must have exactly the same storageset configuration, unit configuration, and physical layout for remote copy sets as the initiator site. Non-RCS LUNs may be different at the two sites.

Create Storage Units

1. Before issuing the following `ADD UNIT` command, you must already have created the required storagesets.

   Issue the following command to create storage units and to disable all access as the units are created.

   `ADD UNIT` *`UnitName StorageSetName`* `DISABLE_ACCESS_PATH=ALL`

Note: If you want to use units that were created with a different `ADD` command, disable all host access to those units by issuing the following command:

`SET` *`UnitName`* `DISABLE_ACCESS_PATH=ALL`

For OpenVMS, set device ID on all units with the following command:

`SET UNIT IDENTIFIER =` *`value`*

Example: `set d1 id = 1`

This becomes the VMS device ID for DGA1.

Issue this command for each unit. After all units have been created, execute the following procedure.

---

2. Set the maximum cached transfer size to 128:

   `SET` *`UnitName`* `MAXIMUM_CACHED_TRANSFER_SIZE = 128`

   Repeat this step for each unit.

Note: We set the maximum cached transfer size to 128 to maximize throughput of initiator-to-target normalization. If a typical application write I/O is larger than 64 kilobytes, then increase MAXIMUM_CACHED_TRANSFER appropriately. See the *HP StorageWorks HSG80 Array Controller Version 8.7 CLI Reference Guide*.

---

3. Verify that the access on each unit is set to NONE:

   ```
   SHOW UNITS FULL
   ```

   You should see a display similar to that in Example Display 9.

Example Display 9

```
LUN                                        Uses             Used by
------------------------------------------------------------------------------
D1                                      DISK10000
   LUN ID:      nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
   NOIDENTIFIER
   Switches:
   RUN                     NOWRITE_PROTECT         READ_CACHE
   READAHEAD_CACHE         WRITEBACK_CACHE
   MAXIMUM_READ_CACHED_TRANSFER_SIZE = 128
  MAXIMUM_WRITE_CACHED_TRANSFER_SIZE = 128
   Access:
   NONE
   State:
   ONLINE to this controller
   NOPREFERRED_PATH
   Size: nnnnnnnn blocks
   Geometry (C/H/S): ( 7000 / 20 / 254 )
.
.
.
```

4. Distribute the units by setting their preferred path:

   ```
   SET UnitName PREFERRED_PATH=THIS_CONTROLLER
   ```

   or

   ```
   SET UnitName PREFERRED_PATH=OTHER_CONTROLLER
   ```

   Keep the busiest units on different controllers.

5. After configuring the units, restart the controllers by issuing the following CLI commands in the order shown. Otherwise, the preferred path settings do not go into effect:

   ```
   RESTART OTHER_CONTROLLER
   RESTART THIS_CONTROLLER
   ```

6. When the controller has restarted, ensure that your storage settings are in place by issuing the following CLI command:

   ```
   SHOW UNITS FULL
   ```

   You should see a display similar to that in Example Display 10.

Example Display 10

```
LUN                                        Uses             Used by
------------------------------------------------------------------------------
D1                                      DISK10000
   LUN ID:      nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
   NOIDENTIFIER
   Switches:
   RUN                     NOWRITE_PROTECT        READ_CACHE
   READAHEAD_CACHE         WRITEBACK_CACHE
   MAXIMUM_READ_CACHED_TRANSFER_SIZE = 128
  MAXIMUM_WRITE_CACHED_TRANSFER_SIZE = 128
   Access:
   NONE
   State:
   ONLINE to this controller
   PREFERRED_PATH = OTHER
   Host based logging NOT specified
  Size: nnnnnnnn blocks
   Geometry (C/H/S): ( 7000 / 20 / 254 )
```

Cable the Target Site

This section provides instructions for cabling the target site.

Connect Fiber Optic Cables Between Controllers and Fibre Channel Switches

Use your established cabling policy to connect the host to the Fibre Channel switches.

1. Make sure that you have installed all required GBICs into each of the Fibre Channel switches.
2. Use 50-micron, multimode fiber optic cable to connect port 1 of the top controller to the top Fibre Channel switch.
3. Use 50-micron, multimode fiber optic cable to connect port 2 of the top controller to the top Fibre Channel switch.
4. Use 50-micron, multimode fiber optic cable to connect port 1 of the bottom controller to the bottom Fibre Channel switch.
5. Use 50-micron, multimode fiber optic cable to connect port 2 of the bottom controller to the bottom Fibre Channel switch.

Tip: You should see an illuminated green LED on the switch as soon as the cable is inserted at both ends. This verifies that there is a good connection.

Example:

a. Insert shortwave GBICs in ports 2 and 4 of both the top and bottom Fibre Channel switches.

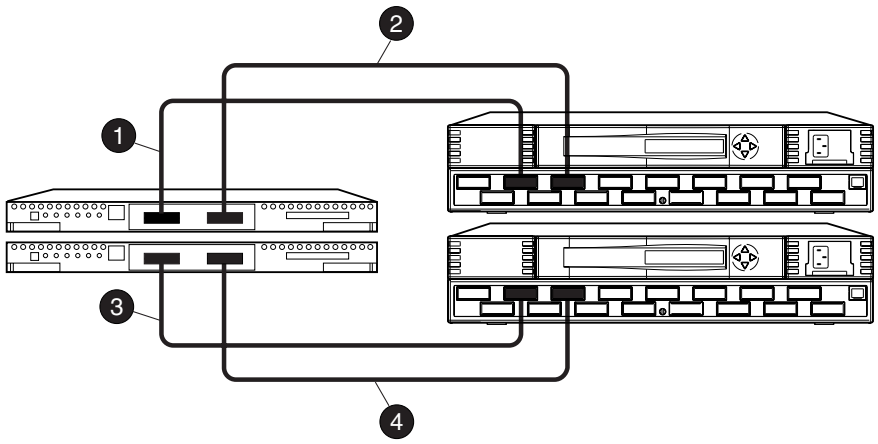
b. Connect a multimode, 50-micron fiber optic cable from port 1 of the top controller to port 2 of the top Fibre Channel switch (as shown by callout 1 in Figure 17).

c. Connect a second multimode, 50-micron fiber optic cable from port 2 of the top controller to port 4 of the top Fibre Channel switch (as shown by callout 2 in Figure 17).

d. Connect a third multimode, 50-micron fiber optic cable from port 1 of the bottom controller to port 2 of the bottom Fibre Channel switch (as shown by callout 3 in Figure 17).

e. Connect a fourth multimode, 50-micron fiber optic cable from port 2 of the bottom controller to port 4 of the bottom Fibre Channel switch (as shown by callout 4 in Figure 17).

Figure 17 illustrates the cabling in the example. In this figure, the controllers are on the left and the switches are on the right.



❶ Cable from port 1 of the top controller to port 2 of the top Fibre Channel switch

❷ Cable from port 2 of the top controller to port 4 of the top Fibre Channel switch

❸ Cable from port 1 of the bottom controller to port 2 of the bottom Fibre Channel switch

❹ Cable from port 2 of the bottom controller to port 4 of the bottom Fibre Channel switch

Figure 17: Cabling between the controllers and the Fibre Channel switches

Connect the Target Site to the External Fiber Link

Locate the offsite connection points at the target site that link the target site to the initiator site.

Execute the procedure in the next section if you have longwave or very long distance GBICs. Otherwise, go the section below titled “Other Transport Modes.”

LongWave or Very Long Distance GBICs

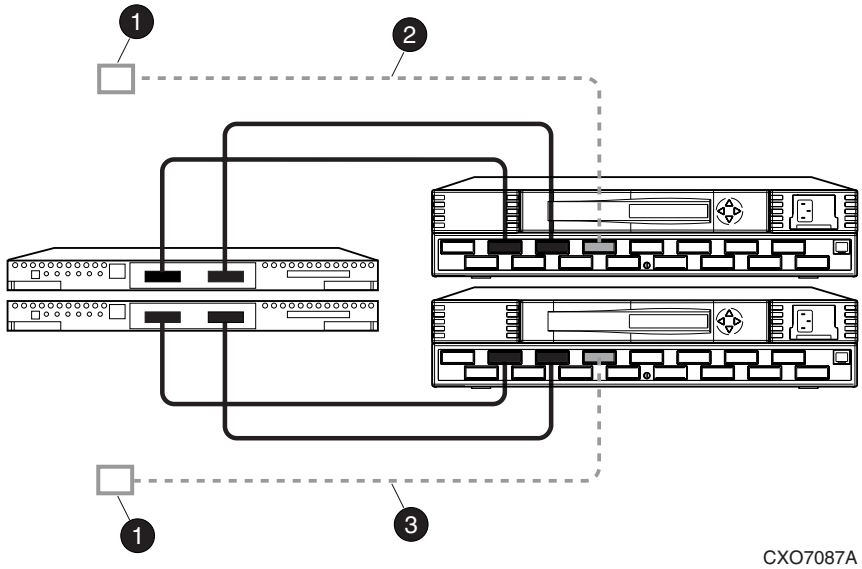
1. Install longwave or very long distance GBIC now if not previously installed.
2. Connect a single-mode, 9-micron fiber optic cable from the longwave or very long distance GBIC in the top switch to one connection point.
3. Connect another single-mode, 9-micron fiber optic cable from the long-wave or very long distance GBIC in the bottom switch to the other connection point.

Other Transport Modes

For a list of the most current software, firmware, patches, drivers, and so on, for each of the supported operating systems in your DRM solution, refer to the DRM Release Notes.

The target site is now physically linked to the initiator site. Figure 18 shows what this cabling should look like.

Note: You can make sure that switches and ports are connected as you have documented them by issuing the `nbrStateShow` switch command. Issue the `topologyShow` command at the switch to reveal whether you have more than one fiber optic cable between the switches on each site.



❶ Connection points to initiator site

❷ Cable from port 6 of the top switch to one connection point

❸ Cable from port 6 of the bottom switch to the other connection point

Figure 18: Cabling from the target site to the initiator site

Create Switch Zones at the Target Site

You must now create zones on the switches that the controllers are connected to. See Chapter 6, "Configuring the Optional Advanced DRM Solutions," for more information on creating zones.

1. Create a zone on the top fabric that contains port 1 of the top controller. This zone will later contain target host connections as well.
2. Create a zone on the top fabric that contains port 2 of the top controller. This zone will be the top ISL zone.
3. Create a zone on the bottom fabric that contains port 1 of the bottom controller. This zone will later contain target host connections as well.
4. Create a zone on the bottom fabric that contains port 2 of the bottom controller. This zone will be the bottom ISL zone.

There must be four zones when you are finished (two per fabric).

Configure the Host at the Target Site

This section describes how to set up your host systems at the target site. Follow the procedures for each operating system in your SAN. Execute the appropriate procedure for each of your operating systems:

- HP OpenVMS, page 74
- HP Tru64 UNIX, page 77
- HP-UX, page 80
- IBM AIX, page 82
- Microsoft Windows NT and Windows 2000, page 90
- Novell NetWare, page 93
- Sun Solaris, page 96

HP OpenVMS

Before beginning this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. Record the HBA World Wide ID (WWID) for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs until instructed to do so.

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide*.

Additional Setup

You will need the latest TIMA kit, which is identified at:

http://h71000.www7.hp.com/openvms/supportchart.html

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   For example, if there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch and the second and fourth adapters must be connected to the bottom Fibre Channel switch.
3. Verify that the connection between the host and the switch has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 11.

Example Display 11

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
!NEWCON00       WINNT           THIS         1        210013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01       WINNT           OTHER        1        200013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like “HostB1.”

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 when renaming your hosts.

!NEWCON*xx*	World Wide Name	Host Name	Host OS Type	HBA Number

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

Figure 19: Host renaming worksheet

2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCON`*`xx`* *`TargetHostConnectionNamex`*

   `RENAME !NEWCON`*`xx`* *`TargetHostConnectionNamey`*

   Example: `rename !NEWCON`*`xx`* `HostB1`

   Example: `rename !NEWCON`*`xx`* `HostB2`

3. Set the operating system for each connection to OpenVMS:

   `SET` *`TargetHostConnectionNamex`* `OPERATING_SYSTEM = VMS`

   Example: `set HostB1 operating_system = vms`

   Example: `set HostB2 operating_system = vms`

4. When you have finished renaming your host connections, issue the following command to see your settings:

   `SHOW CONNECTIONS`

   You should see a display similar to that in Example Display 12.

Example Display 12

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
HostB1     VMS                THIS         1       210013    online  0
   HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HostB2     VMS                 OTHER        1       200013    online  0
   HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on zone creation):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Your OpenVMS host is now configured to use DRM. Execute this procedure for each OpenVMS host present at the target site. After configuring the target site hosts, go to the section titled "Configure the Controllers at the Initiator Site," on page 100.

HP Tru64 UNIX

Before starting this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. Record the HBA WWID for use later in this chapter. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs at this time. The driver is installed in the following step.

Install the HBA Driver

The EMX driver for Tru64 UNIX is already installed. Verify that the driver version and firmware version are at a supported level:

```
cat  /usr/adm/messages |grep KGPSA
```

You should see a display similar to that in Example Display 13.

Example Display 13

```
Apr 19 14:19:37 tru002 vmunix: KGPSA-CA : Driver Rev 1.30:
F/W Rev 3.81A4(2.01A0): wwn 1000-0000-c924-fe8c
```

Multipath Software

Tru64 UNIX has native multipath support with path auto-detection. No further configuration is required.

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide*.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   For example, if there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch and the second and fourth adapters must be connected to the bottom Fibre Channel switch.
3. Verify that the connection between the host and the switch has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 14.

Example Display 14

```
Connection Unit
Name          Operating system   Controller  Port    Address    Status Offset
!NEWCON00      WINNT               THIS        1      210013      online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01      WINNT               OTHER       1      200013      online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like “HostB1.”

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts.
2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCONxx TargetHostConnectionNamex`

   `RENAME !NEWCONxx TargetHostConnectionNamey`

   Example: `rename !NEWCONxx HostB1`

   Example: `rename !NEWCONxx HostB2`
3. Set the operating system for each connection to Tru64 UNIX:

   `SET TargetHostConnectionNamex OPERATING_SYSTEM = TRU64_UNIX`

   Example: `set HostB1 operating_system = tru64_unix`
4. When you have finished renaming your host connections, issue the following command to see your settings:

   `SHOW CONNECTIONS`

   You should see a display similar to that in Example Display 15.

Example Display 15

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
HostB1     Tru64_UNIX THIS         1       210013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HostB2     Tru64_UNIX OTHER        1       200013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on zone creation):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Your Tru64 UNIX host is now configured to use DRM. Execute this procedure for each Tru64 UNIX host present at the target site. After configuring the target site hosts, go to the section titled "Configure the Controllers at the Initiator Site" on page 100.

HP-UX

Before starting this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Existing Fibre Channel HP-UX Configurations

Refer to the current version of the *HP StorageWorks Secure Path for HP-UX Installation and Reference Guide* for information on:

- Changing from SCSI-2 to SCSI-3, Command Console LUN (CCL) behavior
- Changing HBAs and switch modes from QuickLoop to Fabric

This guide is available at:

http://h18006.www1.hp.com/products/sanworks/secure-path/index.html

Install the HBAs

You must install at least two HBAs in each host system. HBAs must be installed in pairs.

Power down your HP-UX host and install the HBAs in any of the free PCI slots. Install the HBA device driver if needed.

Refer to vendor's adapter service and user guide for installation instructions.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switches:

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top fabric.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom fabric.

   For example, if there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch and the second and fourth adapters must be connected to the bottom Fibre Channel switch.

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection on the HSG80. An HBA can be identified by its WWN in the connection description. To find the WWN of each HBA, refer to Chapter 7, “Troubleshooting.”

Initially, each connection on the HSG80 is named !NEWCONxx. It is much easier to track connections if the connection names are meaningful, like "HostB1."

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts. You may reproduce this worksheet as needed.

2. When you have completed the worksheet, rename the connections:

   ```
   RENAME !NEWCONxx TargetHostConnectionNamex
   RENAME !NEWCONxx TargetHostConnectionNamey
   ```

   Example: `rename !NEWCONxx HostB1`

   Example: `rename !NEWCONxx HostB2`

3. Change the operating system for each connection to HP-UX:

   ```
   SET !NEWCONxx operating_system=hp
   ```

4. After you have renamed the host connections, issue the following command to see the new settings:

   ```
   SHOW CONNECTIONS
   ```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information:

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Disable Access to the Hosts at the Target Site

To prevent the target hosts from writing to any remote copy set targets, access must be disabled:

```
SET UnitName DISABLE=ALL
```

Repeat for each unit.

Note: This step is for remote copy set LUNs only.

Install the Secure Path Fibre Channel HBA Device Driver

Install the Secure Path Fibre Channel HBA device driver according to the instructions in the current version of the *HP StorageWorks Secure Path for HP-UX Installation and Reference Guide*.

Verify the Disks

Verify that the nonremote copy set disks are present by issuing the following command:

```
ioscan -fnCdisk
```

The output should be similar to that shown in Example Display 16.

Example Display 16

```
Class    I  H/W Path       Driver S/W State   H/W Type     Description
disk       0  0/0/1/1.2.0    sdisk CLAIMED     DEVICE       SEAGATE ST39204LC
                      /dev/dsk/c1t2d0   /dev/rdsk/c1t2d0
disk       1  0/0/255.0.0.0  sdisk CLAIMED   DEVICE    HSG80 LUN
0x60001FE100080D100009834019820144
                      /dev/dsk/c12t0d0   /dev/rdsk/c12t0d0
```

Note: If the device special files (/dev/dsk/c12t0d0 /dev/rdsk/c12t0d0, for example) are not displayed, then issue the `insf -e` command to install special files, then repeat the `ioscan -fnCdisk` command.

Configure the SWCC Agent (Optional)

⊙ The SWCC Agent may now be installed and configured. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for HP-UX Installation and Configuration Guide,* Chapter 4, for installation instructions.

Additional Setup

⊙ You may now configure volume groups, logical volumes, and file systems on any nonremote copy set LUNs on the storage arrays using normal HP-UX procedures.

Your HP-UX host is now configured to use DRM. Repeat this procedure for each HP-UX host present at your target site. After configuring the target site hosts, go to the section titled "Configure the Controllers at the Initiator Site" on page 100.

IBM AIX

Before starting this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. HBAs must be installed in pairs. You may install a maximum of six adapters per host, but two adapter pairs must not share the same unit on the RAID system.

⊙ Power down your AIX host and install the HBAs in any of the free PCI slots. The HBAs work in either a 32-bit or 64-bit PCI card slot.

Note: Do not attach your fiber connections to the HBAs at this time and do not install the AIX driver that comes with the Cambex HBA. The driver is installed in the following step.

Install the Secure Path Fibre Channel HBA Device Driver and the AIX Platform Kit

The following describes the preferred method for installing the *HP StorageWorks* platform kit software for IBM AIX and Secure Path Fibre Channel HBA device driver software on your AIX servers. Use these instructions, in the given order, instead of the installation instructions in the platform kit (*HP StorageWorks HSG80 ACS Version 8.7 Solution Software for IBM AIX Installation and Configuration Guide)* and Secure Path software *(HP StorageWorks Secure Path for IBM AIX Installation and Reference Guide)*.

New Installation

Follow these instructions if you are performing a new installation of the HP StorageWorks platform kit for AIX and Secure Path.

New Installation Assumptions

- All components are not connected.
- AIX operating system version is v5.1.
- Cambex is the Fibre Channel adapter.
- Secure Path is v2.0D.
- Solution platform kit is v8.7.
- HSG80 ACS code is v8.7P.
- Storage subsystem is pre-configured with or without a CCL LUN.
- Mode is SCSI-2 or SCSI-3, with the LUN connection type set as AIX-Cambex.
- HBAs are installed in pairs.
- No volume groups, logical volumes, or file systems are created.
- Clustering services is not installed.

HBA Limitations

HBAs have the following limitations:

- Addressing of LUNS is limited to 32 devices. This limitation must be considered when planning the sub-system storage configuration.
- Configuring a CCL LUN will leave 31 LUN addresses.

Installation Steps

1. Install Fibre Channel HBAs. Do not connect fiber cables at this time.

Note: The maximum number of HBAs per host is 6. Refer to IBM's PCI Adapter Placement Reference document.

---

2. Power up or boot server.
3. Load the HP StorageWorks HSG80 ACS Version 8.7 platform kit for AIX:
   a. Load platform CD into CD drive.

b. Enter the following commands:

```
#mkdir /cdrom
#mount -v cdrfs -r /dev/cd0 /cdrom
#cd /cdrom
#./INSTALL (follow the prompts)
```

The system will not find any DEC HSG80 RAID array devices at this time.

The option of installing the SWCC Agent will be presented at this time. Choose **Yes**. Installation of the SWCC Agent will begin. When installation is complete, you will be asked if you wish to start the Agent:

- Answer **Yes** if the host will be used as an SWCC Agent.
- Answer **No** if the host will not be used as an SWCC Agent.

Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for IBM AIX Installation and Configuration Guide* for additional information on this process.

```
#umount /cdrom
```

4. Remove platform kit Fibre Channel driver v1.5.20.2 with the following commands:

```
#installp -u PC1000.driver.obj
#lslpp -l PC1000.driver.obj
```

5. Load Secure Path for IBM v2.0D, Fibre Channel driver v1.5.23.2:
   a. Load the Secure Path CD into CD drive.
   b. Enter the following commands:

```
#mkdir /mnt
#mount -v cdrfs -r /dev/cd0 /mnt
#mkdir /tmp/driver
#cp /mnt/driver/PC1000SP.image /tmp/driver
#cd /tmp/driver
#installp -acd PC1000SP.image all
#lslpp -l PC1000.driver.obj
#umount /mnt
```

6. Run Configuration Manger to add the Fibre Channel HBA to the configuration database. Enter the following commands:

```
#cfgmgr -v
#lsdev -Cc adapter
```

7. Connect fiber cables to HBAs.

8. Run Configuration Manager to add hdisks / HSG80 Raid Array to the configuration database. Enter the following commands:

```
#cfgmgr -v
#lsdev -Cc disk
```

The system will find HSG80 Raid Array devices at this time. If CCL is enabled on the HSG80, the server will find a Command Console LUN.

Multiple instances of the Command Console LUN hdisks may be displayed. Remove all of the higher numbered hdisks, keeping only the lowest numbered hdisk of the Command Console LUN. Remove the hdisks with the following command:

```
#rmdev -dl hdiskx
```

where *x* is the number of the hdisk to be removed.

9. Run the StorageWorks Install Agent, if required:

```
#cd /usr/stgwks2
# ./config.sh
```

Choose **Option 3**.

10. Create Volume Groups, Logical Volumes, and File Systems.
11. Configure clustering services (if required).
12. Check the status of the HBAs periodically.

Upgrade Installation

If you are currently using an AIX server in transparent failover mode, and you wish to upgrade to ACS Version 8.7P in a DRM environment, follow these instructions.

Upgrade Installation Assumptions

- All components are connected.
- AIX OS is upgraded to v4.3.3.
- Cambex Fibre Channel adapters are installed.
- A version of Secure Path is loaded.
- A version of the solution platform kit is loaded, or has been upgraded.
- HSG80 ACS code is being upgraded to Version 8.7P.
- Storage subsystem is pre-configured with or without a CCL LUN, in SCSI-2 or SCSI-3 mode, with the LUN connection type set as WINNT.
- HBAs are installed in pairs.
- Volume groups, logical volumes, and file systems created.
- Clustering services may be installed.

HBA Limitations

HBAs have the following limitations:

- Addressing of LUNS is limited to 16 devices. This limitation must be considered when planning the subsystem storage configuration.
- Configuring a CCL LUN will leave 15 LUN addresses.

Installation Steps

1. Stop all I/O.
2. Stop clustering services (if running).
3. Stop the HP StorageWorks Agent (if running).

4. Back up all Volume Groups (highly recommended).
5. Unmount and perform file system check on all logical volumes, varyoff, and export volume groups, with the following commands:

   `#umount /dev/(logical_volume_name)`

   `#fsck /(file_system_name)`

   `#varyoffvg (volume_group_name)`
6. Remove all hdisks associated with DEC HSG80 RAID array from the configuration database with the following commands:

   `#lsdev -Cc disk`

   `#rmdev -dl hdiskx (x is the hdisk number)`
7. Remove all Fibre Channel adapters from the configuration database with the following commands:

   `#lsdev -Cc adapter`

   `#rmdev -dl scsix` (*x* is the Cambex adapter number)
8. Uninstall the Fibre Channel driver with the following command:

   `#installp -u PC1000.driver.obj`
9. Disconnect all Fibre Channel adapter cables.
10. If adding an additional Cambex Fibre Channel adapter, shut down the server with the following command:

    `#shutdown`
11. Install additional Fibre Channel HBAs (if required). Do not connect fiber cables at this time.

Note: The maximum number of HBAs per host is 6. Refer to IBM's PCI Adapter Placement Reference document.

---

12. Power up or boot server.
13. Load StorageWorks HSG80 ACS Version 8.7 platform kit for AIX:
    a. Load platform CD into CD drive.
    b. Enter the following commands:

       `#mkdir /cdrom`

       `#mount -v cdrfs -r /dev/cd0 /cdrom`

       `#cd /cdrom`

       `#./INSTALL` (follow the prompts)

       The system will not find any DEC HSG80 RAID array devices at this time.

The option of installing the SWCC Agent will be presented at this time. Choose **Yes**. Installation of the SWCC Agent will begin. When installation is complete, you will be asked if you wish to start the Agent:

- Answer **Yes** if the host will be used as an SWCC Agent.
- Answer **No** if the host will not be used as an SWCC Agent.

Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for IBM AIX Installation and Configuration Guide* for additional information on this process.

```
#umount /cdrom
```

14. Remove the platform kit Fibre Channel driver with the following commands:

```
#installp -u PC1000.driver.obj
#lslpp -l PC1000.driver.obj
```

15. Load Secure Path for IBM Fibre Channel driver:
    a. Load Secure Path CD into CD drive.
    b. Enter the following commands:

```
#mkdir /mnt
#mount -v cdrfs -r /dev/cd0 /mnt
#mkdir /tmp/driver
#cp /mnt/driver/PC1000SP.image /tmp/driver
#cd /tmp/driver
#installp -acd PC1000SP.image all
#lslpp -l PC1000.driver.obj
#umount /mnt
```

Note: Follow the vendor documentation if using the PC2000 HBA.

16. Run Configuration Manager to add the Fibre Channel HBA to the configuration database with the following commands:

```
#cfgmgr -v
#lsdev -Cc adapter
```

17. Connect fiber cables to HBAs.

18. Run Configuration Manager to add hdisks or HSG80 Raid Array to the configuration database with the following commands:

```
#cfgmgr -v
#lsdev -Cc disk
```

The system will find HSG80 Raid Array devices at this time. If CCL is enabled on the HSG80 the server will find a Command Console LUN.

Multiple instances of the Command Console LUN hdisks may be displayed. Remove all of the higher numbered hdisks, keeping only the lowest numbered hdisk of the Command Console LUN. Remove the hdisks with the following command:

```
#rmdev -dl hdiskx
```

where `x` is the number of the hdisk to be removed.

19. Run the *HP StorageWorks* Install Agent, if required:

    ```
    #cd /usr/stgwks2
    # ./stgwks_aix.sh
    ```

    Choose **Option 1**.

20. Reestablish volume groups, logical volumes, and file systems with the following commands:

    ```
    #varyonvg (volume_group_name)
    #mount /dev/(logical_volume__name)
    ```

21. Reestablish clustering services (if required).

22. Check the status of the HBAs periodically.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switches:

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top fabric.

2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom fabric.

   Example: If there are four adapters in a server, the first and third should be connected to the top fabric; and the second and fourth adapters should be connected to the bottom fabric.

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like “HostB1.”

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts. You may reproduce this worksheet as needed.

2. When you have completed the worksheet, rename the connections:

   ```
   RENAME !NEWCONxx TargetHostConnectionNamex
   RENAME !NEWCONxx TargetHostConnectionNamey
   ```

   Example: `rename !NEWCONxx HostB1`

   Example: `rename !NEWCONxx HostB2`

3. Change the operating system for each connection to AIX (use WINNT for this function):

   ```
   SET  !NEWCONxx  OPERATING_SYSTEM=WINNT
   ```

4. After you have renamed the host connections, issue the following command to see the new settings:

   ```
   SHOW CONNECTIONS
   ```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information:

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Disable Access to the Hosts at the Target Site

To prevent the target hosts from writing to any remote copy set targets, access must be disabled:

```
SET  UnitName  DISABLE=ALL
```

Repeat for each unit.

Note: This step is for remote copy set LUNs only.

Verify the Disks

Verify that disks are present by issuing the following commands:

```
cfgmgr  -v
lsdev  -Cc disk
```

The `cfgmgr` command configures hdisks for all LUNs your system can access on the storage arrays.

The output of the `lsdev` command should be similar to that shown in Example Display 17.

Example Display 17

```
hdisk0 Available 10-60-00-6,0 16 Bit LVD SCSI Disk Drive
hdisk1 Available 20-58-00-8,0 DEC HSG80 Command Console LUN
hdisk2 Available 20-58-00-8,7 DEC HSG80 RAID Array
```

In this example:

- hdisk0 represents the internal hard drive of your AIX host.
- hdisk1 represents the Command Console LUN (CCL).
- hdisk2 represents a single unit or LUN (LUN 7 as denoted by the last number in the line 20-58-00-8,7).

Note: In the example, hdisk2 represents a nonremote copy set because you have disabled access to all RCS LUNs.

Configure the SWCC Agent (Optional)

- The SWCC Agent may now be installed and configured. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for IBM AIX Installation and Configuration Guide* for installation instructions.

Additional Setup

- You may now configure volume groups, logical volumes, and file systems on any nonremote copy set LUNs on the storage arrays using normal AIX procedures.

  Your AIX host is now configured to use DRM. Repeat this procedure for each AIX host present at your target site. After configuring the target site hosts, go to the section titled "Configure the Controllers at the Initiator Site" on page 100.

Microsoft Windows NT and Windows 2000

Before beginning this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Make sure that the hosts are not connected to the Fibre Channel switches during this procedure.

Install the HBAs and Update Firmware

- You must install at least two HBAs in each host system. HBAs must be installed in pairs. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs at this time. The driver is installed in the following step.

Install the HBA Driver

- Use the Device Manager to install the HBA driver. For updated driver version information, refer to the DRM Release Notes.

Install Fibre Channel Software

- Install the HP Fibre Channel software on the host. For updated Fibre Channel software version information, refer to the DRM Release Notes.

Install Multipath Software

Install Secure Path for Windows. For installation instructions, refer to the current version of the *HP StorageWorks Secure Path for Microsoft Windows Installation and Reference Guide* available at http://h18006.www1.hp.com/products/sanworks/secure-path/index.html

1. Verify that the Secure Path Agent is installed by going to **Administrative Tools** and selecting **Services**. The Secure Path Agent must be set for automatic setup and started.
2. Use the *Secure Path Agent Configuration* utility to grant access to the client at both the initiator and target sites. To do this, follow these menus:

   Start > Programs > Secure Path > Secure Path Cfg
3. You can set the password and allow client access via the *Secure Path Agent Configuration* utility.

Note: HP recommends that you set both the fully qualified and unqualified domain name server (DNS) names as valid, authorized clients.

---

4. Restart the Secure Path Agent service for changes to take effect.

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide*.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switches.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each HBA pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   For example, if there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch and the second and fourth adapters must be connected to the bottom Fibre Channel switch.
3. Verify that the connection between the host and the switches has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 18.

Example Display 18

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
!NEWCON00     WINNT             THIS       1      210013     online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01     WINNT             OTHER      1      200013     online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like "HostB1."

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts.
2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCONxx TargetHostConnectionNamex`

   `RENAME !NEWCONxx TargetHostConnectionNamey`

   Example: `rename !NEWCONxx HostB1`

   Example: `rename !NEWCONxx HostB2`
3. Set the operating system for each connection to Windows (NT is the setting for both Windows NT and Windows 2000):

   `SET TargetHostConnectionNamex OPERATING_SYSTEM = WINNT`

   Example: `set HostB1 operating_system = winnt`

   Example: `set HostB2 operating_system = winnt`
4. When you have finished renaming your host connections, confirm your new settings:

   `SHOW CONNECTIONS`

   You should see a display similar to that in Example Display 19.

Example Display 19

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
HostB1          WINNT            THIS        1      210013    online  0
   HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HostB2          WINNT           OTHER        1      200013    online  0
   HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on zone creation):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Your Windows host is now configured to use DRM. Execute this procedure for each Windows host present at the target site. After configuring the target site hosts, go to the section titled "Configure the Controllers at the Initiator Site" on page 100.

Novell NetWare

Before beginning this procedure, make sure that your host is up to date with support packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. Record the HBA WWID for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs until instructed to do so. The driver is installed in the following step.

Install the HBA Driver

The NetWare HBA multipath driver is CPQFC.HAM. The driver is installed as part of the Secure Path Agent installation.

Install Secure Path Agent

For installation instructions, refer to the current version of the *HP StorageWorks Secure Path for Novell NetWare Installation and Reference Guide* located at http://h18006.www1.hp.com/products/sanworks/secure-path/index.html.

After installation, execute the following procedure:

1. Verify that the Secure Path Agent is installed by typing the following at the server console:

   ```
   modules cpqspagt
   ```

   If the agent has installed properly, you will see a display of version information.

   Ensure that the Secure Path Agent is set for automatic startup. Normally, the Secure Path installation program sets automatic startup by loading *cpqspagt.nlm* in the *autoexec.ncf* file.

2. Use the Secure Path Agent Configuration screen at the server to grant access to the client at both the initiator and target sites. To do this:
   a. From the NetWare server, toggle to the Secure Path NLM (NetWare Loadable Module) screen.
   b. At the Main menu, select **2) Client Administration**, then select **2) Add a Client**.
   c. Type the fully qualified DNS name for the client, then press **Enter**.
   d. Press **Esc** to return to the Main menu.
3. To set the password and allow client access via the Secure Path Agent Configuration, execute the following procedure:
   a. At the Main menu, select **1) Agent Administration**, then select **1) Change Password**.
   b. Type a password for client access and then retype the password for verification.
   c. Press **Esc** to return to the Main menu.

Note: HP recommends that you set both the fully qualified and unqualified DNS names as valid, authorized clients.

Install Secure Path Manager

For installation instructions, refer to the current version of the *HP StorageWorks Secure Path for Novell NetWare Installation and Reference Guide*.

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide.*

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   For example, if there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch and the second and fourth adapters must be connected to the bottom Fibre Channel switch.
3. Verify that the connection between the host and the switch has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 20.

Example Display 20

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
!NEWCON00         WINNT       THIS         1      210013     online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01         WINNT       OTHER        1      200013     online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like "HostB1."

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts.
2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCONxx` *`TargetHostConnectionNamex`*

   `RENAME !NEWCONxx` *`TargetHostConnectionNamey`*

   Example: `rename !NEWCONxx HostB1`

   Example: `rename !NEWCONxx HostB2`
3. Set the operating system for each connection to NetWare:

   `SET` *`TargetHostConnectionNamex`* `OPERATING_SYSTEM = NETWARE`

   Example: `set HostB1 operating_system = netware`

   Example: `set HostB2 operating_system = netware`
4. When you have finished renaming your host connections, issue the following command to see your settings:

   `SHOW CONNECTIONS`

   You should see a display similar to that in Example Display 21.

Example Display 21

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
HostB1          NETWARE          THIS        1      210013     online  0
   HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HostB2          NETWARE          OTHER       1      200013     online  0
   HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on zone creation):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Your NetWare host is now configured to use DRM. Execute this procedure for each NetWare host present at the target site. After configuring the target site hosts, go to the section titled "Configure the Controllers at the Initiator Site" on page 100.

Sun Solaris

Before beginning this procedure, make sure that your host is up to date with Solaris operating system patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system and they must be installed in pairs. Record the HBA WWID for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html..

Note: Do not attach your fiber connections to the HBAs until instructed to do so.

WARNING: PCI and Sbus HBAs cannot coexist on the same host.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   For example, if there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch and the second and fourth adapters must be connected to the bottom Fibre Channel switch.

Install the Solaris Platform Kit

Install the Solaris platform kit as specified by the instructions in the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for Sun Solaris Installation and Configuration Guide*. Note that DRM requires the following deviations from the procedures when you install the HBAs:

- **Loop Mode.** Disregard references to Loop Mode. Loop Mode is not supported in DRM.
- **Fabric Mode.** Ensure that the top HBA receives the world wide port number (WWPN) of the corresponding top port 1 address of the controller. Ensure that the bottom HBA receives the WWPN of the corresponding bottom port 1 address of the controller.

Note: The HBA drivers and the SWCC agent are installed in this section. See Table 3-1 in the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for Sun Solaris Installation and Configuration Guide* for a list of installed packages. SWCC is configured (optional) in a later step.

---

1. Reboot the hosts using the `reboot -- -r` command.
2. Verify that the connection between the host and the switch has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 22.

Example Display 22

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
!NEWCON00     WINNT             THIS        1      210013     online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01     WINNT             OTHER       1      200013     online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like "HostB1." We suggest that you use the worksheet in Figure 19 on page 76 to assist in renaming your hosts.

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. When you have completed the worksheet, rename the connections:

   ```
   RENAME !NEWCONxx TargetHostConnectionNamex
   RENAME !NEWCONxx TargetHostConnectionNamey
   Example: rename !NEWCON01 HostB1
   Example: rename !NEWCON02 HostB2
   ```

2. Change the operating system to Solaris for each connection:

   ```
   SET TargetHostConnectionName OPERATING_SYSTEM = SUN
   ```

   Example: `set HostB1 operating_system = sun`

3. When you have finished renaming your host connections, issue the following command to see your settings:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 23.

Example Display 23

```
Connection Unit
Name      Operating system    Controller  Port    Address     Status    Offset
HOSTB1         SUN              THIS         1      210013      online     0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HOSTB2         SUN              OTHER        1      200113      online     0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on zone creation):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Enable Access to the Hosts at the Target Site

The target units must have access to the hosts before configuring Secure Path. Enable access by issuing the following command:

```
SET UnitName ENABLE_ACCESS_PATH = TargetHostConnectionNamex,
TargetHostConnectionNamey
```

Example: `set UnitName enable_access_path = HostB1,HostB2`

Verify the Disks

To run DRM, you must have an even number of HBAs installed in each host system. Follow the procedures outlined here.

1. Reboot the host using the `reboot -- -r` command.
2. Issue the `format` command to verify that the disks are present.

Note: There are two entries for each disk, one per HBA. After installing Secure Path for Solaris, there will be only *one* entry per disk.

Install Secure Path for Solaris Software

Install the Secure Path software as specified in the current version of the *HP StorageWorks Secure Path for Sun Solaris Installation and Reference Guide* available at http://h18006.www1.hp.com/products/sanworks/secure-path/index.html.

After configuring Secure Path, reboot the host using the `reboot -- -r` command.

Reverify the Disks

Issue the `format` command again to verify that disks are present. There must be only one entry for each disk.

Note: All target numbers are stored in *ldLite.conf*.

Configure SWCC Agent (Optional)

You may now configure SWCC. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for Sun Solaris Installation and Configuration Guide* for details on the Configuration utility. Invoke the Configuration utility with the command:

```
/opt/steam/bin/install.h
```

Disable Access to the Hosts at the Target Site

To prevent the target host from writing to any remote copy set targets, disable access by issuing the command:

```
SET UnitName DISABLE=ALL
```

Issue this command for each unit.

Note: This step is for remote copy set (RCS) LUNs only.

Additional Setup

Reboot the host using the `reboot -- -r` command.

The `format` command does not now show any disks from the HSG80 subsystem.

Your Solaris host is now configured to use DRM. Follow this procedure for each Solaris host present at the target site. After configuring the target site hosts, go to the section titled "Configure the Controllers at the Initiator Site" on page 100.

Configure the Controllers at the Initiator Site

Before you configure the controllers at the initiator site, be sure to:

- Identify the WWN on the HBAs.
- Select the name to assign to the initiator site. This name must be different from the one you assigned to the target site.

To get your DT system up and running, you must set up and configure the controllers by executing the following procedure.

1. Ensure that all enclosures, Fibre Channel switches, and power distribution units (PDUs), are powered off.
2. Plug all rack PDU power cords into the main power receptacles.
3. Make sure that you have a serial connection ready to each of the controllers.
4. Power on all PDUs.
5. Ensure that the Fibre Channel switches are powered on, but not cabled.
6. Turn on the enclosures.

Note: When the enclosures are turned on, the controllers will boot only if the PCMCIA cards are installed. If there are no cards in the controller slots, insert them now, and then press the **Reset** button. For complete instructions on how to properly seat the controller cards, refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 Installation and Configuration Guide* for your operating system.

7. Establish a CLI connection to the top controller. Refer to the *HP StorageWorks HSG80 Array Controller ACS V8.7 Maintenance and Service Guide* for instructions.

8. Verify that all controllers are on and functional by observing the CLI prompt on the maintenance port of each controller.

Note: Unless otherwise specified, all operations may be conducted from the top controller (controller A1).

---

9. Verify that the controllers are properly set up:

   ```
   SHOW THIS_CONTROLLER
   ```

   You should see a display similar to that in Example Display 24.

Example Display 24

```
Controller:
            HSG80 ZG8nnnnnnn Software V87P, Hardware  E03
            NODE_ID           = nnnn-nnnn-nnnn-nnnn
            ALLOCATION_CLASS = 0
            SCSI_VERSION      = SCSI-2
            Not configured for dual-redundancy
                Controller misconfigured -- other controller present
            Device Port SCSI address 7
            Time: NOT SET
            Command Console LUN is disabled
            Host connection table is NOT locked
            Smart error eject disabled
    Host PORT_1:
            Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
PORT_1_TOPOLOGY  = OFFLINE (offline)
    Host PORT_2:
            Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
PORT_2_TOPOLOGY  = OFFLINE (offline)
            NOREMOTE_COPY
Cache:
           512 megabyte write cache, version 0012
           Cache is GOOD
           No unflushed data in cache
            CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
 Mirrored Cache:
            Not enabled
Battery:
           FULLY CHARGED
            Expires:
            NOCACHE_UPS
Controller misconfigured. Type SHOW THIS_CONTROLLER
```

10. Verify that the subsystem WWN, also called the *NODE_ID*, is set (if zeros are displayed, the name is not set):
    - If the name is set, go to step 13.
    - If the WWN has not been assigned to the controller, you must obtain the name before proceeding.

Note: The subsystem's WWN and checksum are located on a sticker on top of the frame that houses the controllers, EMU, PVA, and cache modules. This sticker also includes a checksum, which is required to verify that the WWN is valid. If no label is present, contact your HP customer service representative for assistance. For more information on WWNs, refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 Installation and Configuration Guide* for your operating system. Each subsystem's WWN begins with 5000 and ends in zero; for example, 5000-1FE1-FF0C-EE00. The controller port IDs are derived from the WWN.

Caution: Never set two subsystems to the same WWN; data corruption will occur.

11. After the WWN has been located, assign it to the controller:

    `SET THIS_CONTROLLER NODE_ID=`*`node_ID`* `checksum`

    You should see a display similar to that in Example Display 25.

Example Display 25

```
Warning 4000: A restart of this controller is required before all the
   parameters modified will take effect
%CER--HSG80> --09-FEB-1999 10:07:54-- Restart of this controller required
Restart of this controller required
```

12. Issue the `SHOW THIS_CONTROLLER` command to verify that the WWN is set.

    You should see a display similar to that in Example Display 26.

Example Display 26

```
Controller:
            HSG80 ZG8nnnnnnn Software V87-P, Hardware  E03
            NODE_ID           = 5000-nnnn-nnnn-nnn0
            ALLOCATION_CLASS  = 0
            SCSI_VERSION      = SCSI-2
            Not configured for dual-redundancy
                Controller misconfigured -- other controller present
            Device Port SCSI address 7
            Time: NOT SET
            Command Console LUN is disabled
```

13. Configure the controllers for multiple-bus failover mode:

    ```
    SET MULTIBUS_FAILOVER COPY=THIS_CONTROLLER
    ```

    This command automatically restarts the Other controller.

    A `%LFL` and `%EVL` prompt is displayed. Refer to the *HP StorageWorks HSG80 Array Controller ACS V8.7 Maintenance and Service Guide* for more details on these reports.

14. Verify that the setting from step 13 has been applied:

    ```
    SHOW THIS_CONTROLLER FULL
    ```

    Check the display to verify that the controllers have been configured to support multiple-bus failover mode.

    You should see a display similar to that in Example Display 27.

Example Display 27

```
Controller:
            HSG80 ZG8nnnnnnn Software V87-P, Hardware  E03
            NODE_ID          = nnnn-nnnn-nnnn-nnnn
            ALLOCATION_CLASS = 0
            SCSI_VERSION     = SCSI-2
                Configured for MULTIBUS_FAILOVER with ZG8nnnnnnn
                In dual-redundant configuration
            Device Port SCSI address 7
            Time: NOT SET
            Command Console LUN is lun 0 (NOIDENTIFIER)
```

Note: These settings are applied automatically to controller B2. It is not necessary to repeat these steps on controller B2.

---

15. You must select the SCSI mode for the controllers. Some operating systems support only one SCSI mode. For more information, refer to the DRM Release Notes.

    Set SCSI-3 mode:

    ```
    SET THIS SCSI=SCSI-3
    ```

Note: For OpenVMS, set alloclass and identifier:

```
SET THIS ALLOCATION_CLASS = 1
SET THIS IDENTIFIER = 99
```

Setting this switch causes the host to load the SYS$DRIVER, which provides the GG devices. The value range is 1 - 99.

D0 (D-zero) can no longer be used as a device LUN in SCSI-3 mode.

Set SCSI-2 mode:

```
SET THIS SCSI=SCSI-2
```

---

16. Change your controller prompts to identify which controller you are working on:

    SET THIS_CONTROLLER PROMPT="*InitiatorControllerName*Top> "

    SET OTHER_CONTROLLER PROMPT="*InitiatorControllerName*Bottom> "

    Example: set this_controller prompt="BuildingATop> "

    Example: set other_controller prompt="BuildingABottom> "

Note: This step takes effect immediately.

17. Check to see whether mirrored write-back cache is enabled:

    SHOW THIS_CONTROLLER

    If mirrored write-back cache is not enabled, you should see a display similar to that in Example Display 28.

Example Display 28

```
.
.
.
Mirrored Cache:
Not enabled
.
.
.
```

If mirrored write-back cache is not enabled, issue the following CLI command:

SET THIS_CONTROLLER MIRRORED_CACHE

The controllers restart after mirrored write-back cache is set. You should see %LFL and %EVL displays.

Note: It may take up to five minutes after restart for diagnostics to complete on the cache. The controller rejects this command until the cache check is complete. If the command is rejected, do not restart the controllers. Wait a few minutes and then try again.

18. After the controllers restart, confirm that mirrored write-back cache is enabled:

    SHOW THIS_CONTROLLER

    You should see a display similar to that in Example Display 29.

Example Display 29

```
.
.
.
Mirrored Cache:
            256 megabyte write cache, version 0012
            Cache is GOOD
            No unflushed data in cache
.
.
.
```

Note: These settings are applied automatically to controller B2. It is not necessary to repeat these steps on controller B2.

19. Set the fabric topology for each port on both controllers by issuing the following CLI commands:

    Note: You may be prompted to restart the controllers after each command, but you do not need to restart the controllers until all topologies have been set.

    ```
    SET THIS_CONTROLLER PORT_1_TOPOLOGY=FABRIC
    SET THIS_CONTROLLER PORT_2_TOPOLOGY=FABRIC
    SET OTHER_CONTROLLER PORT_1_TOPOLOGY=FABRIC
    SET OTHER_CONTROLLER PORT_2_TOPOLOGY=FABRIC
    ```

20. Issue the following CLI command:

    ```
    SET LOG NOLOG
    ```

    Note: You can ignore the error message `ERROR B020:No Logdisk is Configured` if it appears.

21. Restart the controllers in the order shown:

    ```
    RESTART OTHER_CONTROLLER
    RESTART THIS_CONTROLLER
    ```

    Note: There may be a brief delay before control is returned.

22. After the controllers have restarted, verify that the topology is set correctly:

    ```
    SHOW THIS_CONTROLLER
    SHOW OTHER_CONTROLLER
    ```

    You should see a display similar to that in Example Display 30.

Example Display 30

```
.
.
.
Host PORT_1:
   Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
    . . . . . . . . . . . . . . . . . . . PORT_1_TOPOLOGY  = FABRIC (up)
Host PORT_2:
   Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
    . . . . . . . . . . . . . . . . . . .PORT_2_TOPOLOGY  = FABRIC (up)
   NOREMOTE_COPY
```

23. You are now ready to enable DRM. Issue the following CLI command:

    `SET THIS_CONTROLLER REMOTE_COPY=`*`InitiatorControllerName`*

    Example: `set this_controller remote_copy=BuildngA`

Note: Be sure to specify a meaningful *InitiatorControllerName,* such as a name that reflects the initiator node's location. Do not use "local" or "remote"; they are reserved keywords. The name can be up to eight characters and must be unique to all of your controllers.

After entering this CLI command, you should see a series of `%LFL` and `%EVL` displays; the controllers automatically restart.

24. Verify that these settings are in place:

    `SHOW THIS_CONTROLLER`

    You should see a display similar to that in Example Display 31.

Example Display 31

```
.
.
.
Host PORT_2:
            Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
            PORT_2_TOPOLOGY  = FABRIC (offline)
            REMOTE_COPY = BUILDNGA
.
.
.
```

Configure Storage at the Initiator Site

This section explains how to configure storage for remote replication.

Devices and Storagesets

Before you can configure the storage for remote replication, you must add disks, create storagesets, and create units. Follow the instructions in the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 Installation and Configuration Guide* for your operating system, but note the restrictions listed in Table 6 on page 58 of this document.

Note: D0 (D-zero) can no longer be used as a device LUN in SCSI-3 mode.

The target site must have exactly the same storageset configuration, unit configuration, and physical layout for remote copy sets as the initiator site. Non-RCS LUNs may be different at the two sites.

Create Storage Units

Before issuing this `ADD UNIT` command, you must already have created any storagesets required. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 Installation and Configuration Guide*, for your operating system, for detailed information on configuring units.

1. Issue the following command to create storage units and to disable all access as the units are being created.

   `ADD UNIT` *`UnitName StorageSetName`*

2. If you want to use units that were created with a different `ADD` command, disable all host access to those units by issuing the following command:

   `SET` *`UnitName`* `DISABLE_ACCESS_PATH=ALL`

   Repeat this step for each unit.

Note: For OpenVMS, set device ID on all units:

`SET UNIT IDENTIFIER =` *`value`*

Example: `set d1 id = 1`

This becomes the VMS device ID for DGA1.

3. After all units have been created, verify that the access on each unit is set to NONE:

   ```
   SHOW UNITS FULL
   ```

   You should see a display similar to that in Example Display 32.

Example Display 32

```
LUN                                        Uses             Used by
------------------------------------------------------------------------
D10   . . . . . . . . . . . . . . . . . . . . . . . . . . . . DISK1000
   LUN ID:      nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
NOIDENTIFIER
Switches:
RUN . . . . . . . . . . . . . . . . . . . .NOWRITE_PROTECT READ_CACHE‘
READAHEAD_CACHE . . . . . . . . . . . . . . . . . . . .WRITEBACK_CACHE
MAXIMUM_CACHED_TRANSFER_SIZE = 32
   Access:
    NONE
   State:
    ONLINE to this controller
    Not reserved
    NOPREFERRED_PAT
   Size: nnnnnnnn blocks
    Geometry (C/H/S): ( 7000 / 20 / 254 )
.
.
```

4. Distribute the units by setting their preferred path. Use either of the following CLI commands:

   ```
   SET UnitName PREFERRED_PATH=THIS_CONTROLLER
   ```

   or

   ```
   SET UnitName PREFERRED_PATH=OTHER_CONTROLLER
   ```

5. After configuring the units, restart the controllers in the order shown (otherwise, the preferred path settings will not go into effect):

   ```
   RESTART OTHER_CONTROLLER
   RESTART THIS_CONTROLLER
   ```

6. When the controllers have restarted, ensure that your storage settings are in place:

   ```
   SHOW UNITS FULL
   ```

   You should see a display similar to that in Example Display 33.

Example Display 33

```
LUN                                        Uses             Used by
------------------------------------------------------------------------
D10   . . . . . . . . . . . . . . . . . . . . . . . . . . . . DISK1000
   LUN ID:      nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
NOIDENTIFIER
Switches:
RUN . . . . . . . . . . . . . . . . . . . .NOWRITE_PROTECT READ_CACHE‘
READAHEAD_CACHE . . . . . . . . . . . . . . . . . . . .WRITEBACK_CACHE
MAXIMUM_CACHED_TRANSFER_SIZE = 32
   Access:
    NONE
   State:
    ONLINE to this controller
    Not reserved
    PREFERRED_PATH = THIS
   Host based logging NOT specified
     Size: nnnnnnnn blocks
    Geometry (C/H/S): ( 7000 / 20 / 254 )
.
```

Cable the Initiator Site

This section explains how to cable controllers and switches at the initiator site.

Connect Fiber Optic Cables Between Controllers and Fibre Channel Switches

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Make sure that you have installed all required GBICs into each of the Fibre Channel switches.
2. Use 50-micron, multimode fiber optic cable to connect port 1 of the top controller to the top Fibre Channel switch.
3. Use 50-micron, multimode fiber optic cable to connect port 2 of the top controller to the top Fibre Channel switch.
4. Use 50-micron, multimode fiber optic cable to connect port 1 of the bottom controller to the bottom Fibre Channel switch.
5. Use 50-micron, multimode fiber optic cable to connect port 2 of the bottom controller to the bottom Fibre Channel switch.

Note: You should see an illuminated green LED on the switch as soon as the cable is inserted at both ends. This verifies that there is a good connection.

Example:

a. Insert short-wave GBICs in ports 2 and 4 of the top and bottom Fibre Channel switches.

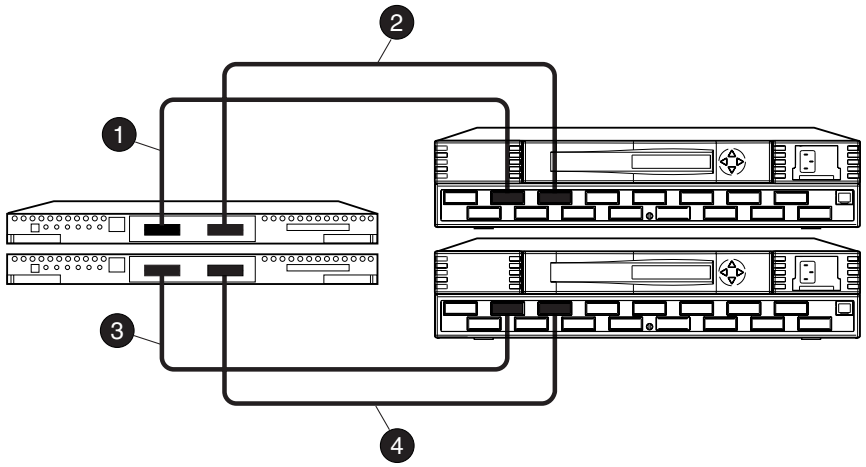
b. Connect a 50-micron, multimode fiber optic cable from port 1 of the top controller to port 2 of the top Fibre Channel switch (as shown by callout 1 of Figure 20).

c. Connect a second 50-micron, multimode fiber optic cable from port 2 of the top controller to port 4 of the top Fibre Channel switch (as shown by callout 2 of Figure 20).

d. Connect a third 50-micron, multimode fiber optic cable from port 1 of the bottom controller to port 2 of the bottom Fibre Channel switch (as shown by callout 3 of Figure 20).

e. Connect a fourth 50-micron, multimode fiber optic cable from port 2 of the bottom controller to port 4 of the bottom Fibre Channel switch (as shown by callout 4 of Figure 20).

Figure 20 illustrates this example. In this figure, the controllers are on the left and the switches are on the right.



❶ Cable from port 1 of the top controller to port 2 of the top Fibre Channel switch

❷ Cable from port 2 of the top controller to port 4 of the top Fibre Channel switch

❸ Cable from port 1 of the bottom controller to port 2 of the bottom Fibre Channel switch

❹ Cable from port 2 of the bottom controller to port 4 of the bottom Fibre Channel switch

Figure 20: Cabling between the controllers and the Fibre Channel switches

Connect the Initiator Site to the External Fiber Link

Locate the connection points at the initiator site that link the initiator site to the target site. Execute the procedure in the next section if you have longwave or very long distance GBICs. Otherwise, go the section titled "Other Transport Modes," on page 111.

Longwave or Very Long Distance GBICs

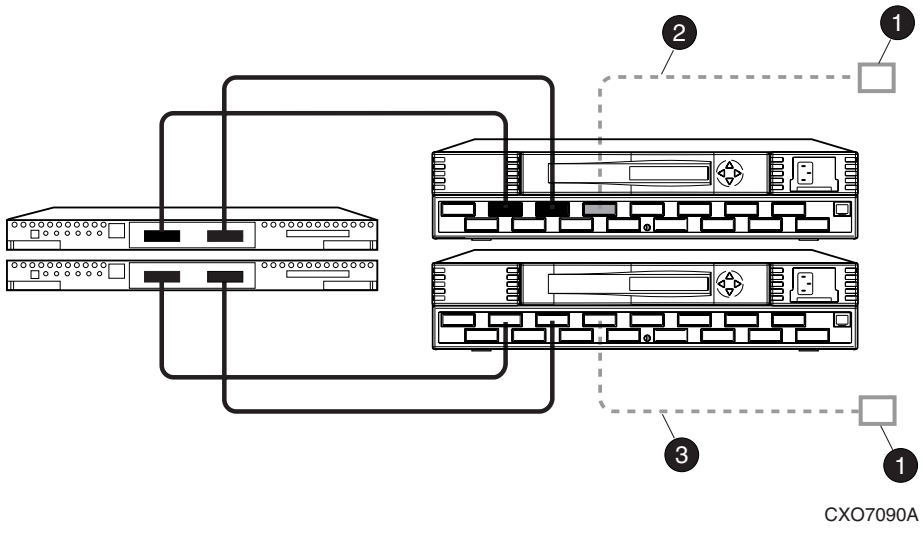
1. Install longwave or very long distance GBIC now if not previously installed.
2. Connect a single-mode, 9-micron fiber optic cable from the longwave or very long distance GBIC in the top switch to one connection point.
3. Connect another single-mode, 9-micron fiber optic cable from the longwave or very long distance GBIC in the bottom switch to the other connection point.

Other Transport Modes

For a list of the most current software, firmware, patches, drivers, and so on, for each of the supported operating systems in your DRM solution, refer to the DRM Release Notes.

The initiator site is now physically linked to the target site. See Figure 21 for a diagram of the cabling.

Note: You can verify that switches and ports are connected as you have documented them by issuing the `nbrStateShow` switch command. Issue the `topologyShow` switch command to reveal whether you have more than one fiber optic cable between the switches at each site.



❶ Connection points to target site

❷ Cable from port 6 of the top switch to one connection point

❸ Cable from port 6 of the bottom switch to the other connection point

Figure 21: Cabling from the initiator to the target site

Create Switch Zones

Switch zones must now be created and updated. See Chapter 6, "Configuring the Optional Advanced DRM Solutions," for more information on creating zones.

1. Create a zone on the top fabric that contains port 1 of the top controller. This zone will later contain initiator host connections as well.
2. Add port 2 of the top controller to the top ISL zone created at the target site. This zone must now contain port 2 of the initiator controller and port 2 of the target controller.
3. Create a zone on the bottom fabric that contains port 1 of the bottom controller. This zone will later contain initiator host connections as well.
4. Add port 2 of the bottom controller to the bottom ISL zone created at the target site. This zone must now contain port 2 of the initiator controller and port 2 of the target controller.

There should now be a total of six zones (three per fabric). There must be two ISL zones (one per fabric), two initiator host zones (one per fabric), and two target host zones (one per fabric).

Note: If any target hosts will be using nonremote copy sets on the initiator, they must be added to the zones in step 1 and step 3.

Create Remote Copy Sets

This section explains how to establish remote copy sets (RCSs).

Prepare the Initiator Site

Before creating the RCS, create the connections between the initiator and target sites by issuing the following CLI command:

```
ADD REMOTE RCS200 D200 TargetControllerName\D200
```

Example: `add remote rcs200 d200 BuildngB\D200`

Note: This command fails (because a unit number must be in the range 0 through 199), and the following error message is displayed: `Initiator unit specified not found`. However, it does properly create and name the connections.

Create Connections from the Target Site

1. Before creating the remote copy set, create the connections between the target and initiator sites:

   ```
   ADD REMOTE RCS200 D200 InitiatorControllerName\D200
   ```

   Example: `add remote rcs200 d200 BuildngA\D200`

Note: This command fails, and the following error message is displayed: `Initiator unit specified not found`. However, it does create and name the connections.

---

2. Verify that the target has access to the initiator controller:

   ```
   SHOW CONNECTIONS
   ```

   This command shows all the connections; verify that the following are included: *InitiatorControllerA, InitiatorControllerB, InitiatorControllerC, InitiatorControllerD.*

3. The target units must allow access to the controllers at the initiator site. Enable access with the following CLI command:

   ```
   SET UnitName ENABLE_ACCESS_PATH=(InitiatorControllerConnectionA,
   InitiatorControllerConnectionB, InitiatorControllerConnectionC,
   InitiatorControllerConnectionD)
   ```

   Example: `set d1 enable_access_path=(BuildngAA, BuildngAB, BuildngAC, BuildngAD)`

   Repeat this command for each UnitName.

4. Issue a `SHOW UNITS FULL` command to verify that the correct access path has been created for each unit.

Create Remote Copy Sets from the Initiator Site

1. Verify that the initiator has access to the target controller:

   ```
   SHOW CONNECTIONS
   ```

   This command shows all the connections; verify that the following are included: *TargetControllerA, TargetControllerB, TargetControllerC, TargetControllerD.*

2. The initiator controllers must have access to the controllers at the target site. Enable access by issuing the following CLI command:

   ```
   SET UnitName ENABLE_ACCESS_PATH=(TargetControllerConnectionA,
   TargetControllerConnectionB, TargetControllerConnectionC,
   TargetControllerConnectionD)
   ```

   Example: `set d1 enable_access_path=(BuildngBA, BuildngBB, BuildngBC, BuildngBD)`

   Note: Repeat this command for each UnitName.

3. To create remote copy sets, issue the CLI command below. When you issue this command, the controllers copy all data from the initiator unit to the target unit. This process is called *normalization*.

   Note: Remote copy set names are limited to alphanumeric characters, the underscore, and the hyphen.

   ```
   ADD REMOTE RemoteCopySetName initiatorUnitName
   TargetControllerName\TargetUnitName
   ```

   Example: `add remote rcs1 d1 BuildngB\D1`

   Repeat this step for all units that you want to become remote copy sets. It is not necessary to repeat this step at the target site.

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

Repeat for each remote copy set.

You will see a confirmation message on your terminal, as shown in Example Display 34. If the instance code on your screen matches the instance code in this example, you have performed this command correctly.

Example Display 34

```
%EVL--Initra > --13-JAN-1946 05:01:56 (time not set)-- Instance Code: 0E010064
  Template: 144.(90)
  Power On Time: 0. Years, 36. Days, 6. Hours, 45. Minutes, 22. Seconds
  Controller Model: HSG80
  Serial Number: ZG8nnnnnnn Hardware Version:  Enn(2B)
  Software Version: V87P
  Informational Report
  Target Controller Board Serial Number: "      ZG8nnnnnnn"
  Initiator WWLID: nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
  Initiator Node Name: "BuildngA"
  Initiator Unit Number: n.(nnnnnnnn)
  Target WWLID: nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
  Target Node Name: "BuildngB"
  Target Unit Number: n.(nnnnnnnn)
  Remote Copy Set Name: "RCS1”
  Instance Code: 0E010064
```

Set Failsafe at the Initiator Site (Optional)

When Failsafe mode is set and the remote copy set loses the target member, no further I/O is allowed to the initiator member and an error is returned to the host. This is known as a *failsafe locked* condition.

1. If you choose to set Failsafe mode, issue the following command:

   `SET RemoteCopyName ERROR_MODE=FAILSAFE`

   Example: `Set rcs1 error_mode=failsafe`

Note: When you set failsafe, all remote copy sets must be in a normal or normalizing state. If remote copy sets are copying when you set failsafe, your command is rejected until the remote copy sets return to normal mode.

2. To remove the failsafe lock from a remote copy set and resume normal operation, issue the following CLI command:

   `SET RemoteCopyName ERROR_MODE=NORMAL`

   Example: `set rcs1 error_mode=normal`

You can also use this procedure for remote copy sets where a disaster-tolerant (DT) condition is not required.

Note: If the error mode is set to normal and there is no target member, the remote copy set is no longer considered DT.

Create Write History Log Units and Association Sets (Optional)

In the examples in this section, hypothetical disks 50100 and 60100 are the mirrorset for the log disk. The write history log unit is MIR_D1LOG. The association set name is AS_D1. The association set uses remote copy set name RCS1.

Create a Write History Log Unit

1. Create a mirrorset for the write history log disk:

   `ADD MIRRORSET MirrorsetName DiskName1 DiskName2`

   Example: `add mirrorset mir_d1log disk50100 disk60100`

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

To minimize the number of devices used for logging, you can create and use one-member mirrorsets. The logged data is not protected because it is written only to one disk. However, all of this data is also written to the initiator unit. In the case of a log disk failure, you would incur a full normalization, rather than a mini-merge, when access to the target is reestablished. The command to create a one-member mirrorset is the same as that above, except only one disk is listed. Example: `ADD MIRRORSET MIR_D1LOG DISK 50100.`

---

2. Initialize the mirrorset:

   `INITIALIZE MirrorsetName`

   Example: `initialize mir_d1log`

3. Verify that you have created a mirrorset:

   `SHOW StoragesetType`

   Example: `show mir_d1log`

   You should see a display similar to that in Example Display 35.

Example Display 35

```
Name          Storageset         Uses           Used by
------------------------------------------------------------------------
MIR_D1LOG     mirrorset          DISK50100       DISK60100
```

4. Present the log unit to the controller:

   `ADD UNIT` *`UnitName MirrorsetName`*

   Example: `add unit d10 mir_d1log`

5. Verify that the controller recognizes the log unit:

   `SHOW UNITS`

   You should see a display similar to that in Example Display 36.

Example Display 36

```
LUN                                    Uses             Used by
------------------------------------------------------------------------
D10                                 MIR_D1LOG
```

Create Association Sets and Assign a Write History Log Unit

1. Create an association set:

   `ADD ASSOCIATIONS` *`AssociationSetName RemoteCopySetName`*

   Example: `add associations as_d1 rc_d1`

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

You can add additional members to the association set by issuing the following CLI command: SET *AssociationSetName* ADD=*RemoteCopySetName*

---

2. Disable node access to the write history log unit:

   `SET` *`UnitNumber`* `DISABLE_ACCESS_PATH= ALL`

   Example: `set d10 disable_access_path= all`

3. Disable mirrored write-back cache on write history log units:

   `SET` *`UnitNumber`* `NOWRITEBACK_CACHE`

   Example: `set d10 nowriteback_cache`

4. Verify that you have disabled access and mirrored write-back cache:

   `SHOW` *`UnitNumber`*

   Example: `show d10`

   You should see a display similar to that in Example Display 37.

Example Display 37

```
LUN                                          Uses             Used by
---------------------------------------------------------------------
D10                                           MIR_D1LOG
LUN ID:      6000-1FE1-0001-3B10-0009-9130-8044-0066
IDENTIFIER = 10
Switches:
RUN                    NOWRITE_PROTECT        READ_CACHE
READAHEAD_CACHE        NOWRITEBACK_CACHE
MAXIMUM_CACHED_TRANSFER_SIZE = 32
Access:
    None
State:
   ONLINE to this controller
   Not reserved
   PREFERRED_PATH = THIS_CONTROLLER
  Host based logging NOT specified
Size:             35556389 blocks
Geometry (C/H/S): ( 7000 / 20 / 254 )
```

5. Assign the write history log unit to the association set:

   `SET AssociationSetName LOG_UNIT = D10`

   Example: `set as_d1 log_unit = d10`

Note: If you choose to set the fail_all property of the association set, make sure that all of the remote copy sets in the association are set to failsafe error mode. If you do this, however, you will not be able to use a write history log unit.

---

6. Check to see the switch status of the association set:

   `SHOW AssociationSetName`

   Example: `show as_d1`

   You should see a display similar to that in Example Display 38.

Example Display 38

```
Name          Association                    Uses             Used by
-------------------------------------------------------------------------
AS_D1       association                    RC_D1
Switches:
  NOFAIL_ALL
  NOORDER_ALL
  LOG_UNIT = D10 (No data logged)
```

7. You may set the FAIL_ALL or ORDER_ALL properties of the association set now, if desired, by issuing the following CLI commands:

```
SET AssociationSetName FAIL_ALL
SET AssociationSetName ORDER_ALL
```

Note: If you choose to set the FALL_ALL property of the association set, make sure that all of the remote copy sets in the association set are set to failsafe error mode. If you choose to use failsafe error mode, you cannot use a log unit.

Configure the Host at the Initiator Site

This section describes how to set up your host systems at the initiator site. Follow the procedures for each operating system present in your SAN:

- HP OpenVMS, page 118
- HP Tru64 UNIX, page 121
- HP-UX, page 123
- IBM AIX, page 126
- Microsoft Windows NT and Windows 2000, page 134
- Novell NetWare, page 137
- Sun Solaris, page 141

HP OpenVMS

Before beginning this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. Record the HBA WWID for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs until instructed to do so.

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide.*

Additional Setup

You will need the latest TIMA kit, which is identified at:
http://h71000.www7.hp.com/openvms/supportchart.html

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   Example: If there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch; the second and fourth adapters must be connected to the bottom Fibre Channel switch.
3. Verify that the connection between the host and the switch has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 39.

Example Display 39

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
!NEWCON00    VMS               THIS        1       210013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01    VMS               OTHER       1       200013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify the hosts, HP recommends that you rename the host connections using a meaningful name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is easier to track connections if the connection names are meaningful, like “HostA1.”

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming hosts.

2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCONxx InitiatorHostConnectionNamex`

   `RENAME !NEWCONxx InitiatorHostConnectionNamey`

   Example: `rename !NEWCONxx HostA1`

   Example: `rename !NEWCONxx HostA2`

3. Set the operating system for each connection to OpenVMS:

   `SET InitiatorHostConnectionNamex OPERATING_SYSTEM=VMS`

   Example: `set HostA1 operating_system = vms`

   Example: `set HostA2 operating_system = vms`

4. When you have finished naming your host connections, issue the following command to verify your new settings:

   `SHOW CONNECTIONS`

   You should see a display similar to that in Example Display 40.

Example Display 40

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
HostA1      VMS THIS          1       210013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HostA2      VMS OTHER         1       200013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created at the target site must be updated with the host connection information (refer to Chapter 6, “Configuring the Optional Advanced DRM Solutions,” for detailed information on zone creation):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top initiator controller.

2. On the bottom fabric, add the host connection to the zone that contains port 1 of bottom the initiator controller.

Enable Access to the Hosts at the Initiator Site

The initiator units must have access to the hosts. Enable access with the following CLI command:

`SET UnitName ENABLE_ACCESS_PATH=(InitiatorHostConnectionNamex, InitiatorHostConnectionNamey)`

Example: `set unitname enable_access_path=(HostA1,HostA2)`

Repeat this step for all units.

Your OpenVMS host is now configured to use DRM. Follow this procedure for each OpenVMS host present at the initiator site. After configuring the initiator site hosts, go to the section titled “Additional Host Configuration,” on page 144.

HP Tru64 UNIX

Before beginning this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. Record the HBA WWID for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs until instructed to do so. The driver is installed in the following step.

Install the HBA Driver

The EMX driver for Tru64 UNIX is already installed. Issue the following command to verify that the driver version and the firmware version are at supported levels:

```
#  cat  /usr/adm/messages  lgrep  KGPSA
```

You should see a display similar to that in Example Display 41.

Example Display 41

```
Apr 19 14:19:37 tru002 vmunix: KGPSA-CA : Driver Rev 1.30 :
F/W Rev 3.81A4(2.01A0): wwn 1000-0000-c924-fe8c
```

Multipath Software

Tru64 UNIX has native multipath support with path auto-detection. No further configuration is required.

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide.*

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   Example: If there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch. The second and fourth adapters must be connected to the bottom Fibre Channel switch.
3. Verify that the host has logged into the fabric:

   ```
   SHOW CONNECTIONS
   ```

You should see a display similar to that in Example Display 42.

Example Display 42

```
Connection Unit
Name       Operating system   Controller  Port    Address    Status Offset
!NEWCON00   WINNT              THIS        1       210013     online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01   WINNT              OTHER       1       200013     online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify the hosts you are working with, HP recommends that you rename the host connections using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like "HostA1."

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. Use the worksheet in Figure 19 on page 76 to assist in renaming your hosts.
2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCONxx` *`InitiatorHostConnectionNamex`*

   `RENAME !NEWCONxx` *`InitiatorHostConnectionNamey`*

   Example: `rename !NEWCONxx HostA1`

   Example: `rename !NEWCONxx HostA2`
3. Set the operating system for each connection to Tru64 UNIX:

   `SET` *`TargetHostConnectionName`* `OPERATING_SYSTEM=TRU64_UNIX`

   Example: `set HostA1 operating_system=tru64_unix`
4. When you have finished renaming your host connections, verify your settings:

   `SHOW CONNECTIONS`

   You should see a display similar to that in Example Display 43.

Example Display 43

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
HostA1     Tru64_UNIX THIS         1       210013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HostA2     Tru64_UNIX OTHER        1       200013    online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created at the target site must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on zone creation):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top initiator controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom initiator controller.

Enable Access to the Hosts at the Initiator Site

1. The initiator units must have access to the hosts. Enable access with the following command:

   `SET` *`UnitName`* `ENABLE_ACCESS_PATH=`*`InitiatorHostConnectionNamex, InitiatorHostConnectionNamey`*

   Example: `set` *`UnitName`* `enable_access_path=HostA1,HostA2`

Note: There must be two paths per host. Repeat this sequence for each host.

---

2. From a terminal window on the host, issue the following commands to recognize the new units and assign device special file numbers:

   ```
   # hwmgr - scan comp - cat scsi_bus
   # hwmgr - show scsi
   ```

Your Tru64 UNIX host is now configured to use DRM. Follow this procedure for each Tru64 UNIX host present at the initiator site. After configuring the initiator site hosts, go to the section titled "Additional Host Configuration," on page 144.

HP-UX

Before starting this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Existing Fibre Channel HP-UX Configurations

Refer to the current version of the *HP StorageWorks Secure Path for HP-UX Installation and Reference Guide* for information on:

- Changing from SCSI-2 to SCSI-3, Command Console LUN (CCL) behavior
- Changing HBAs and switch modes from QuickLoop to Fabric

Install the HBAs

You must install at least two HBAs in each host system. HBAs must be installed in pairs.

Power down your HP-UX host and install the HBAs in any of the free PCI slots. Install the HBA device driver if needed.

Refer to vendor's adapter service and user guide for installation instructions.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switches:

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top fabric.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom fabric.

   Example: If there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch. The second and fourth adapters must be connected to the bottom Fibre Channel switch.

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection on the HSG80. An HBA can be identified by its WWN in the connection description. To find the WWN of each HBA, refer to Chapter 7, “Troubleshooting.”

Initially, each connection on the HSG80 is named !NEWCONxx. It is much easier to track connections if the connection names are meaningful, like "HostA1."

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. Use the worksheet in Figure 19 on page 76 to assist in renaming your hosts. You may reproduce this worksheet as needed.
2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCONxx` *`TargetHostConnectionNamex`*

   `RENAME !NEWCONxx` *`TargetHostConnectionNamey`*

   Example: `rename !NEWCONxx HostA1`

   Example: `rename !NEWCONxx HostA2`

3. Change the operating system for each connection to HP-UX:

   ```
   SET !NEWCONxx operating_system=hp
   ```

4. After you have renamed the host connections, issue the following command to see the new settings:

   ```
   SHOW CONNECTIONS
   ```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information:

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Enable Access to the Hosts at the Initiator Site

The initiator hosts must have access to the units. Enable access with the following command:

```
SET UnitName ENABLE_ACCESS_PATH=InitiatorHostConnectionNamex,
InitiatorHostConnectionNamey
```

Example: `set UnitName enable_access_path=HostA1,HostA2`

Repeat this step for each unit.

Install the Secure Path Fibre Channel HBA Device Driver

Install the Secure Path Fibre Channel HBA device driver according to the instructions in the current version of the *HP StorageWorks Secure Path for HP-UX Installation and Reference Guide.*

Verify the Disks

1. Verify that the disks are present by issuing the following command:

   ```
   ioscan -fnCdisk
   ```

The output should be similar to that shown in Example Display 44.

Example Display 44

```
Class    I  H/W Path    Driver S/W State   H/W Type     Description
disk 0   0/0/1/1.2.0    sdisk CLAIMED      DEVICE       SEAGATE ST39204LC
                 /dev/dsk/c1t2d0   /dev/rdsk/c1t2d0
disk 1   0/0/255.0.0.0  sdisk CLAIMED      DEVICE HSG80 LUN
0x60001FE100080D100009834019820144
                 /dev/dsk/c8t0d0   /dev/rdsk/c8t0d0
```

Note: If the device special files (that is, /dev/dsk/c8t0d0, /dev/rdsk/c8t0d0) are not displayed, then issue command `insf -e` to install special files and repeat the command `ioscan -fnCdisk`.

Configure the SWCC Agent (Optional)

You may now install and configure the SWCC Agent. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for HP-UX Installation and Configuration Guide* for installation instructions.

Additional Setup

You may now configure volume groups, logical volumes, and file systems on any nonremote copy set LUNs on the storage arrays using normal HP-UX procedures.

Your HP-UX host is now configured to use DRM. Repeat this procedure for each HP-UX host present at your initiator site. After configuring the initiator site hosts, go to the section titled "Additional Host Configuration," on page 144.

IBM AIX

Before beginning this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. HBAs must be installed in pairs. You may install a maximum of six adapters per host, but two adapter pairs must not share the same unit on the RAID system.

Power down your AIX host and install the HBAs in any of the free PCI slots. The HBAs work in either a 32-bit or 64-bit PCI card slot. Record the HBA WWID for use later in this section.

Note: Do not attach your fiber connections to the HBAs at this time and do not install the AIX driver that comes with the Cambex HBA. The driver is installed in the following step.

Install the Secure Path Fibre Channel HBA Driver and the AIX Platform Kit

The following describes the preferred method for installing the *StorageWorks* platform kit software for IBM AIX and Secure Path Fibre Channel HBA device driver software on your AIX servers. Use these instructions, in the given order, instead of the installation instructions in the platform kit (*HP StorageWorks HSG80 ACS Version 8.7 Solution Software for IBM AIX Installation and Configuration Guide)* and Secure Path software (*HP StorageWorks Secure Path for IBM AIX Installation and Reference Guide)*.

New Installation

Follow these instructions if you are performing a new installation of the HP StorageWorks platform kit for AIX and Secure Path.

New Installation Assumptions

- All components are not connected.
- AIX operating system version is v4.3.3 or v5.1
- Cambex is the Fibre Channel adapter.
- Latest version of Secure Path software.
- Solution platform kit is v8.7.

- HSG80 ACS code is v8.7P.
- Storage subsystem is pre-configured with or without a CCL LUN.
- Mode is SCSI-2 or SCSI-3, with the LUN connection type set as WINNT.
- HBAs are installed in pairs.
- No volume groups, logical volumes, or file systems are created.
- Clustering services is not installed.

HBA Limitations

HBAs have the following limitations:

- Addressing of LUNS is limited to 16 devices. This limitation must be considered when planning the subsystem storage configuration.
- Configuring a CCL LUN will leave 15 LUN addresses.

Installation Steps

1. Install Fibre Channel HBAs. Do not connect fiber cables at this time.

Note: The maximum number of HBAs per host is 6. Refer to IBM's PCI Adapter Placement Reference document.

---

2. Power up or boot server.
3. Load the HP StorageWorks HSG80 ACS Version 8.7 platform kit for AIX:
   a. Load platform CD into CD drive.
   b. Enter the following commands:

```
#mkdir /cdrom
#mount -v cdrfs -r /dev/cd0 /cdrom
#cd /cdrom
#./INSTALL (follow the prompts)
```

   The system will not find any DEC HSG80 RAID array devices at this time.

   The option of installing the SWCC Agent will be presented at this time. Choose **Yes**. Installation of the SWCC Agent will begin. When installation is complete, you will be asked if you wish to start the Agent:

   - Answer **Yes** if the host will be used as an SWCC Agent.
   - Answer **No** if the host will not be used as an SWCC Agent.

   Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for IBM AIX Installation and Configuration Guide* for additional information on this process.

```
#umount /cdrom
```

4. Remove platform kit Fibre Channel driver with the following commands:

```
#installp -u PC1000.driver.obj
#lslpp -l PC1000.driver.obj
```

5. Load Secure Path for IBM Fibre Channel driver:
   a. Load the Secure Path CD into the CD drive.
   b. Enter the following commands:

```
#mkdir /mnt
#mount -v cdrfs -r /dev/cd0 /mnt
#mkdir /tmp/driver
#cp /mnt/driver/PC1000SP.image /tmp/driver
#cd /tmp/driver
#installp -acd PC1000SP.image all
#lslpp -l PC1000.driver.obj
#umount /mnt
```

Note: Follow the vendor documentation if using the PC2000 HBA.

6. Run Configuration Manager to add Fibre Channel HBA to the configuration database. Enter the following commands:

```
#cfgmgr -v
#lsdev -Cc adapter
```

7. Connect fiber cables to HBAs.

8. Run Configuration Manager to add hdisks / HSG80 Raid Array to the configuration database. Enter the following commands:

```
#cfgmgr -v
#lsdev -Cc disk
```

   The system will find HSG80 Raid Array devices at this time. If CCL is enabled on the HSG80 the server will find a Command Console LUN.

   Multiple instances of the Command Console LUN hdisks may be displayed. Remove all of the higher numbered hdisks, keeping only the lowest numbered hdisk of the Command Console LUN. Remove the hdisks with the following command:

```
#rmdev -dl hdiskx
```

   where x is the number of the hdisk to be removed.

9. Run the HP StorageWorks Install Agent, if required:

```
#cd /usr/stgwks2
# ./stgwks_aix.sh
```

   Choose **Option 1**.

10. Create Volume Groups, Logical Volumes, and Files Systems.

11. Configure clustering services (if required).

12. Check the status of the HBAs periodically.

Upgrade Installation

If you are currently using an AIX server in transparent failover mode, and you wish to upgrade to ACS Version 8.7P in a DRM environment, follow these instructions.

Upgrade Installation Assumptions

- All components are connected
- AIX OS is upgraded to v4.3.3 or v5.1
- Cambex Fibre Channel adapters are installed
- A version of Secure Path is loaded
- A version of the solution platform kit is loaded, or has been upgraded
- HSG80 ACS code is being upgraded to v8.7P
- Storage subsystem is pre-configured with or without a CCL LUN, in SCSI-2 or SCSI-3 mode, with the LUN connection type set as WINNT
- HBAs are installed in pairs
- Volume groups, logical volumes, and file systems created
- Clustering services may be installed

HBA Limitations

HBAs have the following limitations:

- Addressing of LUNS is limited to 16 devices. This limitation must be considered when planning the subsystem storage configuration.
- Configuring a CCL LUN will leave 15 LUN addresses.

Installation Steps

1. Stop all I/O.
2. Stop clustering services (if running).
3. Stop the HP StorageWorks Agent (if running).
4. Backup all Volume Groups (highly recommended).
5. Unmount and perform file system check on all logical volumes, varyoff, and export volume groups, with the following commands:

   ```
   #umount /dev/(logical_volume_name)
   #fsck /(file_system_name)
   #varyoffvg (volume_group_name)
   ```

6. Remove all hdisks associated with DEC HSG80 RAID array from the configuration database with the following commands:

   ```
   #lsdev -Cc disk
   #rmdev -dl hdiskx (x is the hdisk number)
   ```

7. Remove all Fibre Channel adapters from the configuration database with the following commands:

   ```
   #lsdev -Cc adapter
   #rmdev -dl scsix (x is the Cambex adapter number)
   ```

8. Uninstall the Fibre Channel driver with the following command:

   ```
   #installp -u PC1000.driver.obj
   ```

9. Disconnect all Fibre Channel adapter cables.

10. If adding an additional Cambex Fibre Channel adapter, shut down the server with the following command:

    ```
    #shutdown
    ```

11. Install additional Fibre Channel HBAs (if required). Do not connect fiber cables at this time.

Note: The maximum number of HBAs per host is 6. Refer to IBM's PCI Adapter Placement Reference document.

---

12. Power up or boot server.

13. Load HP StorageWorks platform kit for AIX v8.7:

    a. Load platform CD into CD drive.

    b. Enter the following commands:

    ```
    #mkdir /cdrom
    #mount -v cdrfs -r /dev/cd0 /cdrom
    #cd /cdrom
    #./INSTALL (follow the prompts)
    ```

    The system will not find any DEC HSG80 RAID array devices at this time.

    The option of installing the SWCC Agent will be presented at this time. Choose **Yes**. Installation of the SWCC Agent will begin. When installation is complete, you will be asked if you wish to start the Agent:

    - Answer **Yes** if the host will be used as an SWCC Agent.
    - Answer **No** if the host will not be used as an SWCC Agent.

    Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for IBM AIX Installation and Configuration Guide* for additional information on this process.

    ```
    #umount /cdrom
    ```

14. Remove platform kit Fibre Channel driver with the following commands:

    ```
    #installp -u PC1000.driver.obj
    #lslpp -l PC1000.driver.obj
    ```

15. Load Secure Path for IBM Fibre Channel driver:

    a. Load the Secure Path CD in to the CD drive.

b. Enter the following commands:

```
#mkdir /mnt
#mount -v cdrfs -r /dev/cd0 /mnt
#mkdir /tmp/driver
#cp /mnt/driver/PC1000SP.image /tmp/driver
#cd /tmp/driver
#installp -acd PC1000SP.image all
#lslpp -l PC1000.driver.obj
#umount /mnt
```

16. Run `Configuration Manger` to add Fibre Channel HBA to the configuration database with the following commands:

```
#cfgmgr -v
#lsdev -Cc adapter
```

17. Connect fiber cables to HBAs.

18. Run `Configuration Manager` to add hdisks or HSG80 Raid Array to the configuration database with the following commands:

```
#cfgmgr -v
#lsdev -Cc disk
```

The system will find HSG80 Raid Array devices at this time. If CCL is enabled on the HSG80 the server will find a Command Console LUN.

Multiple instances of the Command Console LUN hdisks may be displayed. Remove all of the higher numbered hdisks, keeping only the lowest numbered hdisk of the Command Console LUN. Remove the hdisks with the following command:

```
#rmdev -dl hdiskx
```

where `x` is the number of the hdisk to be removed.

19. Run the HP StorageWorks Install Agent, if required:

```
#cd /usr/stgwks2
# ./stgwks_aix.sh
```

Choose **Option 1**.

20. Re-establish volume groups, logical volumes, and files systems with the following commands:

```
#varyonvg (volume_group_name)
#mount /dev/(logical_volume__name)
```

21. Reestablish clustering services (if required).

22. Check the status of the HBAs periodically.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switches:

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top fabric.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom fabric.

   Example: If there are four adapters in a server, the first and third should be connected to the top fabric; and the second and fourth adapters should be connected to the bottom fabric.

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like "HostA1."

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts.
2. When you have completed the worksheet, rename the connections:

   ```
   RENAME !NEWCONxx TargetHostConnectionNamex
   RENAME !NEWCONxx TargetHostConnectionNamey
   ```

   Example: `rename !NEWCONxx HostA1`

   Example: `rename !NEWCONxx HostA2`
3. Change the operating system for each connection to IBM AIX (use WINNT for this function):

   ```
   SET  !NEWCONxx  operating_system=WINNT
   ```
4. After you have renamed the host connections, verify the new settings:

   ```
   SHOW CONNECTIONS
   ```

Update Switch Zones

The switch zones created earlier must be updated with the host connection information:

1. On the top fabric, add the host connection to the zone that contains port 1 of the top target controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom target controller.

Enable Access to the Hosts at the Initiator Site

The initiator hosts must have access to the units. Enable access with the following command:

```
SET  UnitName  ENABLE_ACCESS_PATH=InitiatorHostConnectionNamex,
InitiatorHostConnectionNamey
```

Example: `set UnitName enable_access_path=HostA1,HostA2`

Repeat this step for each unit.

Verify the Disks

Verify that disks are present by issuing the following commands:

```
cfgmgr  -v
lsdev  -Cc disk
```

The `cfgmgr` command configures hdisks for all LUNs that your system can access on the storage arrays.

The output of the `lsdev` command should be similar to that shown in Example Display 45.

Example Display 45

```
hdisk0 Available 10-60-00-6,0 16 Bit LVD SCSI Disk Drive
hdisk1 Available 20-58-00-8,0 DEC HSG80 Command Console LUN
hdisk2 Available 20-58-00-8,7 DEC HSG80 RAID Array
```

In this example:

- hdisk0 represents the internal hard drive of your AIX host.
- hdisk1 represents the Command Console LUN (CCL).
- hdisk2 represents a single unit or LUN (LUN 7 as denoted by the last number in the line 20-58-00-8,7).

Configure the SWCC Agent (Optional)

The SWCC Agent may now be installed and configured. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for IBM AIX Installation and Configuration Guide* for installation instructions.

Additional Setup

You may now configure volume groups, logical volumes, and file systems on the storage arrays using normal AIX procedures.

Your AIX host is now configured to use DRM. Repeat this procedure for each AIX host present at the initiator site. After configuring the initiator site hosts, go to the section titled “Additional Host Configuration,” on page 144.

Microsoft Windows NT and Windows 2000

Before beginning this procedure, make sure that your host is up to date with service packs and patches. For supported revision levels, refer to the DRM Release Notes.

Ensure that the hosts are not connected to the Fibre Channel switches at any point during this procedure.

Install the HBAs

You must install at least two HBAs in each host system. HBAs must be installed in pairs. Record the HBA WWID for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at:
http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs until instructed to do so. The driver is installed in the following step.

Install the HBA Driver

Use Device Manager to install the HBA driver. For updated driver version information, refer to the DRM Release Notes.

Install Fibre Channel Software

Install the HP Fibre Channel software on the host. For updated Fibre Channel software version information, refer to the DRM Release Notes.

Install Multipath Software

Secure Path must be installed on the host at this point. For installation instructions, refer to the current version of the *HP StorageWorks Secure Path Version for Microsoft Windows Installation and Reference Guide.*

1. Verify that the Secure Path Agent is installed by going to **Administrative Tools** and selecting **Services**. The Secure Path Agent must be set for automatic setup and started.
2. Use the *Secure Path Agent Configuration* utility to grant access to the client at both the initiator and target sites. To do this, follow these menus:

   Start > Programs > Secure Path > Secure Path Cfg.
3. You can set the password and allow client access via the *Secure Path Agent Configuration* utility.

Note: HP recommends that you set both the fully qualified and unqualified DNS names as valid, authorized clients.

---

4. Restart the Secure Path Agent service for changes to take effect.

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide.*

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   For example, if there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch and the second and fourth adapters must be connected to the bottom Fibre Channel switch.
3. Verify that the connection between the host and the switch has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 46.

Example Display 46

```
Connection Unit
Name      Operating system    Controller   Port   Address    Status Offset
!NEWCON00      WINNT             THIS         1      210013     online   0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01      WINNT             OTHER        1      200113     online   0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON03      WINNT             THIS         1      nnnnnn     online   0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON04      WINNT             OTHER        1      nnnnnn     online   0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like “HostA1.”

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts.

2. When you have completed the worksheet, rename the connections:

   RENAME !NEWCON*xx TargetHostConnectionNamex*

   RENAME !NEWCON*xx TargetHostConnectionNamey*

   Example: rename !NEWCON*xx* HostA1

   Example: rename !NEWCON*xx* HostA2

3. Set the operating system for each connection to Windows:

   SET *TargetHostConnectionNamex* OPERATING_SYSTEM = WINNT

   Example: set HostA1 operating_system = winnt

   Example: set HostA2 operating_system = winnt

4. When you have finished renaming your host connections, verify your new settings:

   SHOW CONNECTIONS

   You should see a display similar to that in Example Display 47.

Example Display 47

```
Connection Unit
Name      Operating system    Controller   Port   Address    Status Offset
BUILDNGBA PPRC_TARGET      THIS      2             online 0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBB PPRC_TARGET      OTHER     2  . . . . . . . . . . . online 0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBC PPRC_INITIATOR   THIS      2  . . . . . . . . . . . online 0
HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBD PPRC_INITIATOR   OTHER     2  . . . . . . . . . . . online 0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HOSTA1      WINNT              THIS         1      210013     online   0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HOSTA2      WINNT              OTHER        1      200113     online   0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
.
.
.
```

Update Switch Zones

The switch zones created at the target site must be updated with the host connection information (refer to Chapter 6, “Configuring the Optional Advanced DRM Solutions,” for detailed information on zone creation and updating switch zones):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top initiator controller.

2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom initiator controller.

Your Windows host is now configured to use DRM. Execute this procedure for each Windows host present at the initiator site. After configuring the initiator site hosts, go to the section titled “Additional Host Configuration,” on page 144.

Novell NetWare

Before beginning this procedure, make sure that your host is up to date with support packs and patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. Record the HBA WWID for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at: http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs until instructed to do so. The driver is installed in the following step.

Install the HBA Driver

The NetWare HBA multipath driver is CPQFC.HAM. The driver is installed as part of the Secure Path Agent installation. Refer to the next section.

Install Secure Path Agent

For installation instructions, refer to the current version of the *HP StorageWorks Secure Path Version for Novell NetWare Installation and Reference Guide*. After installation, execute the following procedure:

1. Verify that the Secure Path Agent is installed by typing the following at the server console:

   ```
   modules cpqspagt
   ```

   If the agent has installed properly, you will see a display of version information.

   Ensure that the Secure Path Agent is set for automatic startup. Normally, the Secure Path installation program sets automatic startup by loading *cpqspagt.nlm* in the *autoexec.ncf* file.

2. Use the Secure Path Agent Configuration screen at the server to grant access to the client at both the initiator and target sites. To do this:
   a. From the NetWare server, toggle to the Secure Path NLM (NetWare Loadable Module) screen.
   b. At the Main menu, select **2) Client Administration**, then select **2) Add a Client**.
   c. Type the fully qualified DNS name for the client, then press **Enter**.
   d. Press **Esc** to return to the Main menu.

3. To set the password and allow client access via the Secure Path Agent Configuration, execute the following procedure:
   a. At the Main menu, select **1) Agent Administration**, then select **1) Change Password**.
   b. Type a password for client access and then retype the password for verification.
   c. Press **Esc** to return to the Main menu.

Note: HP recommends that you set both the fully qualified and unqualified DNS names as valid, authorized clients.

Install Secure Path Manager

For installation instructions, refer to the current version of the *HP StorageWorks Secure Path for Novell NetWare Installation and Reference Guide.*

Install SWCC (Optional)

You may now install SWCC. For detailed information about SWCC, including installation, refer to the *Compaq StorageWorks Command Console Version 2.4 User Guide.*

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   For example, if there are two adapters in a server, the first adapter must be connected to the top Fibre Channel switch and the second adapter must be connected to the bottom Fibre Channel switch.
3. Verify that the connection between the host and the switch has been made:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 48.

Example Display 48

```
Connection Unit
Name       Operating system     Controller Port    Address   Status Offset
!NEWCON00      WINNT              THIS       1       210013   online   0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01      WINNT              OTHER      1       200113   online   0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBA PPRC_TARGET      THIS     2 . . . . . . . . . . . . online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBB PPRC_TARGET       OTHER    2  . . . . . . . . . . . online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBCPPRC_INITIATOR    THIS     2   . . . . . . . . . . . online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBDPPRC_INITIATOR    OTHER    2   . . . . . . . . . . . online 0
  HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections, using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like "HostA1."

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts.
2. When you have completed the worksheet, rename the connections:

   `RENAME !NEWCONxx TargetHostConnectionNamex`

   `RENAME !NEWCONxx TargetHostConnectionNamey`

   Example: `rename !NEWCONxx HostA1`

   Example: `rename !NEWCONxx HostA2`
3. Set the operating system for each connection to NetWare:

   `SET TargetHostConnectionNamex OPERATING_SYSTEM = NETWARE`

   Example: `set HostA1 operating_system = netware`

   Example: `set HostA2 operating_system =  netware`
4. When you have finished renaming your host connections, verify your settings:

   `SHOW CONNECTIONS`

   You should see a display similar to that in Example Display 49.

Example Display 49

```
Connection Unit
Name       Operating system     Controller Port    Address   Status Offset
HOSTA1      NETWARE              THIS       1      210013     online   0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HOSTA2      NETWARE              OTHER      1      200113     online   0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBA PPRC_TARGET            THIS       2 . . . . . . . . online   0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBB PPRC_TARGET        OTHER   2 . . . . . .online 0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBCPPRC_INITIATOR      THIS    2 . . . . . .online 0
OST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
BUILDNGBDPPRC_INITIATOR      OTHER   2 . . . . . .online 0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Update Switch Zones

The switch zones created at the target site must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on creating and updating switch zones):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top initiator controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom initiator controller.

Enable Access to the Hosts at the Initiator Site

1. The initiator units must have access to the hosts. Enable access with the following command:

   `SET` *`UnitName`* `ENABLE_ACCESS_PATH=`*`InitiatorHostConnectionNamex, InitiatorHostConnectionNamey`*

   Example: `set` *`UnitName`* `enable_access_path=HostA1,HostA2`

   Note: There must be two paths per host. Repeat this sequence for each host.

2. After you have enabled host access to units, issue the following command from the NetWare server console prompt:

   `SCAN FOR NEW DEVICES`

3. Use ConsoleOne to create traditional partitions and volumes, or use Novell Storage Services (NSS) partitions, pools, and logical volumes on the newly-created storage.
4. From the server console prompt, type:

   `MOUNT ALL (for traditional volumes)`

   or

   `MOUNT` *`VolumeName`* `(for NSS logical volumes)`

5. You are now ready to run Secure Path Manager from your Windows NT or Windows 2000 client machine. Click: **Start > Programs > Secure Path > SPM.** Specify the server and password.
6. The Secure Path Manager screen appears. Click each drive icon. The device properties appear in the right pane. Ensure that each drive can be moved successfully between controllers by right-clicking the icon and selecting **Move to Other Controller**.

Your NetWare host is now configured for DRM. Follow this procedure for each NetWare host present at the initiator site. After configuring the initiator site hosts, go to the section titled "Additional Host Configuration," on page 144.

Sun Solaris

Before beginning this procedure, make sure that your host is up to date with Solaris OS patches. For supported revision levels, refer to the DRM Release Notes.

Install the HBAs

You must install at least two HBAs in each host system. HBAs must be installed in pairs. Record the HBA WWID for use later in this section. Refer to the *Compaq StorageWorks 64-Bit PCI-to-Fibre Channel Host Bus Adapter User Guide* for installation instructions. The user guide is located at:
http://h18004.www1.hp.com/products/storageworks/techdoc/adapters/AA-RKPDB-TE.html.

Note: Do not attach your fiber connections to the HBAs until instructed to do so.

WARNING: PCI and Sbus HBAs cannot coexist on the same host.

Connect the Host to the SAN

Use your established cabling policy to connect the host to the Fibre Channel switch.

1. Use 50-micron, multimode fiber optic cable to connect one adapter of each pair to the top Fibre Channel switch.
2. Use 50-micron, multimode fiber optic cable to connect the other adapter of each pair to the bottom Fibre Channel switch.

   Example: If there are four adapters in a server, the first and third adapters must be connected to the top Fibre Channel switch; the second and fourth adapters must be connected to the bottom Fibre Channel switch.

Install the Solaris Platform Kit

1. Install the Solaris platform kit following the instructions in the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for Sun Solaris Installation and Configuration Guide*. Note that DRM requires the following deviations from the steps in this procedure:
   - **Loop Mode.** Disregard references to Loop Mode. Loop Mode is not supported in DRM.
   - **Fabric Mode.** Ensure that the top HBA receives the world wide port number (WWPN) of the corresponding top port 1 address of the controller, and that the bottom HBA receives the WWPN of the corresponding bottom port 1 address of the controller.

Note: Install the HBA drivers and the SWCC agent in this step. See the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for Sun Solaris Installation and Configuration Guide* for the list of installed packages. Configure SWCC (as an option) in a later step.

2. Reboot the host using the `reboot -- -r` command.

3. Verify that the host has logged into the fabric:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 50.

Example Display 50

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status Offset
!NEWCON00    WINNT              THIS       1       210013      online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
!NEWCON01    WINNT              OTHER      1       200013      online  0
  HOST_ID=nnnn-nnnn-nnnn-nnnn   . . . . ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, HP recommends that you rename the host connections using a meaningful connection name for each. Each HBA appears as a connection. An HBA can be identified by its WWN, which you recorded when you installed the HBAs, and which appears in the connection description.

Initially, each connection is named !NEWCON*xx*. It is much easier to track connections if the connection names are meaningful, like "HostA1." We suggest that you use the worksheet in Figure 19 on page 76 when renaming your hosts.

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

---

1. When you have completed the worksheet, rename the connections:

   ```
   RENAME !NEWCON01 InitiatorHostConnectionNamex
   RENAME !NEWCON02 InitiatorHostConnectionNamey
   ```

   Example: `rename !NEWCONxx HostA1`

   Example: `rename !NEWCONxx HostA2`

2. Set the operating system for each connection to Solaris:

   ```
   SET InitiatorHostConnectionNamex OPERATING_SYSTEM = SUN
   ```

   Example: `set HostA1 operating_system = sun`

3. When you have finished renaming your host connections, verify your new settings:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 51.

Example Display 51

```
Connection Unit
Name      Operating system    Controller  Port    Address    Status   Offset
HOSTA1       SUN                 THIS       1       210013     online   0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
HOSTA2       SUN                 OTHER      1       200113     online   0
   HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
.
.
.
```

Update Switch Zones

The switch zones created at the target site must be updated with the host connection information (refer to Chapter 6, "Configuring the Optional Advanced DRM Solutions," for detailed information on updating switch zones):

1. On the top fabric, add the host connection to the zone that contains port 1 of the top initiator controller.
2. On the bottom fabric, add the host connection to the zone that contains port 1 of the bottom initiator controller.

Enable Access to the Hosts at the Initiator Site

The initiator units must have access to the hosts. Enable access with the following command:

`SET UnitName ENABLE_ACCESS_PATH=InitiatorHostConnectionNamex, InitiatorHostConnectionNamey`

Example: `set UnitName enable_access_path=HostA1,HostA2`

Repeat this step for all units.

Verify the Disks

To run DRM, you must have an even number of HBAs installed in each host system. Follow the procedures below:

1. Reboot the host using the `reboot -- -r` command.
2. Issue the `format` command to verify that disks are present.

Note: There are two entries for each disk, one per HBA. After installing Secure Path for Solaris, there will be only *one* entry per disk.

Install Secure Path for Solaris Software

Install the Secure Path software as specified in the current version of the *HP StorageWorks Secure Path for Sun Solaris Installation and Reference Guide.*

Configure Secure Path with the following command:

```
/opt/CPQswsp/bin/spconfig -o -p /kernel/drv
```

After installing Secure Path, reboot the host using the `reboot -- -r` command.

Reverify the Disks

Issue the `format` command again to verify that disks are present. There must be only one entry for each disk.

Note: All target numbers are stored in ldLite.conf.

Configure the SWCC Agent (Optional)

You may now install SWCC. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 for Sun Solaris Installation and Configuration Guide* for details regarding the *Configuration* utility.

Invoke the *Configuration* utility with the following command:

```
/opt/steam/bin/install.sh
```

Additional Setup

Reboot the host using the `reboot -- -r` command.

Your Solaris host is now configured to use DRM. Follow this procedure for each Solaris host present at the initiator site. After configuring the initiator site hosts, go to the section titled "Additional Host Configuration," on page 144.

Additional Host Configuration

This section provides the final configuration procedures, which are to be performed at both the initiator and target sites. The procedures are marked with both symbols: ▷⊙.

Install Cluster Server for Windows NT and Windows 2000 (Optional)

▷⊙

Windows NT and Windows 2000 Fibre Channel cluster software enables two host servers to share a Fibre Channel storage subsystem through a Fibre Channel switch. If a failure occurs on the server, the cluster software detects that failure and initiates a failover. The failed components can be warm-swapped or serviced while the functioning components remain active. This process requires minimal downtime and ensures high availability of data. If you are using Windows NT or Windows 2000 and want to run the cluster option, you may safely install it now.

Install NetWare Cluster Services (NWCS) Version 1.01 (Optional)

▷⊙

NWCS Fibre Channel cluster software enables two host servers to share a Fibre Channel storage subsystem through a Fibre Channel switch. If a failure occurs on the server, the cluster software detects that failure and initiates a failover. The failed components can be warm-swapped or serviced while the functioning components remain active. This process requires minimal downtime and ensures high availability of data. If you are using NetWare 5.1 and want to run the cluster option, you may safely install it now.

Only non-RCS LUNs are supported.

Documenting Your Configuration

Keep a copy of both configurations at both sites. Update your records whenever you modify the configuration. Follow the steps outlined below in the sections titled "Terminal Emulator Session" and "SHOW Commands" to obtain a status of the controllers, association sets, remote copy sets, units, and connections. After you have obtained this information for the initiator site, repeat the steps for the target site.

Terminal Emulator Session

1. Connect a serial cable between a computer's serial port and the HSG80 serial port. The computer can be a desktop or laptop with at least one open serial port.
2. Start a terminal emulator session and connect to the controller. The default connection settings for the controllers are 9600 baud, 8 bits, no parity, 1 stop bit.
3. From the Transfer menu, click **Capture Text**. In the c:\ field of the Capture Text dialog box, type `initiator.txt` or `target.txt`.
4. Click **Start**.

SHOW Commands

Note: `SHOW` commands are discussed in detail in Appendix A.

1. To see the full information on this controller, issue the following CLI command:

   ```
   SHOW THIS_CONTROLLER FULL
   ```

   You should see a display similar to that in Example Display 52.

Example Display 52

```
Controller:
        HSG80 ZG91412410 Software S050P-0, Hardware  E05
        NODE_ID          = 5000-1FE1-0001-3AE0
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-3
        Configured for MULTIBUS_FAILOVER with ZG91416136
            In dual-redundant configuration
        Device Port SCSI address 6
        Time: NOT SET
        Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
        Reported PORT_ID = 5000-1FE1-0001-3AE1
        PORT_1_TOPOLOGY  = FABRIC (fabric up)
        Address          = 220113
Host PORT_2:
        Reported PORT_ID = 5000-1FE1-0001-3AE2
```

```
        PORT_2_TOPOLOGY  = FABRIC (fabric up)
        Address          = 220313
        REMOTE_COPY = BuildngA
Cache:
        256 megabyte write cache, version 0012
        Cache is GOOD
        No unflushed data in cache
        CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
Mirrored Cache:
        256 megabyte write cache, version 0012
        Cache is GOOD
        No unflushed data in cache
Battery:
        NOUPS
        FULLY CHARGED
        Expires:
Extended information:
        Terminal speed 9600 baud, eight bit, no parity, 1 stop bit
            Operation control: 00000000  Security state code: 75184
            Configuration backup disabled
```

2. To see the information for all association sets known to the controller pair, issue the following CLI command:

   ```
   SHOW ASSOCIATIONS FULL
   ```

   You should see a display similar to that in Example Display 53 for each association set.

Example Display 53

```
    Name          Association                   Uses             Used by
    ------------------------------------------------------------------------
    AS1           association                   RC1
                                                RC2
                                                RC3
            Switches:
              NOFAIL_ALL
              NOORDER_ALL
              NOLOG_UNIT
```

3. To see information for all remote copy sets known to the controller pair, issue the following CLI command:

   ```
   SHOW REMOTE_COPY_SETS FULL
   ```

   You should see a display similar to that in Example Display 54 for each remote copy set.

Example Display 54

```
Name                                              Uses             Used by
------------------------------------------------------------------------
RC1           remote copy                         D1               AS1
        Reported LUN ID: 6000-1FE1-0001-3AE0-0009-9141-6136-0038
        Switches:
          OPERATION_MODE  = SYNCHRONOUS
          ERROR_MODE      = NORMAL
          FAILOVER_MODE   = MANUAL
          OUTSTANDING_IOS = 60
        Initiator (BuildngA\D1)
        State:
          ONLINE to this controller
        Target state:
         BuildngB\D1 is NORMAL
```

4. To see information for all units configured to the controller, issue the following CLI command:

   ```
   SHOW UNITS FULL
   ```

   You should see a display similar to that in Example Display 55 for each unit.

Example Display 55

```
D2                                          DISK10100 BuildngA\RC2
        LUN ID:      6000-1FE1-0001-3AE0-0009-9141-6136-0045
        NOIDENTIFIER
        Switches:
          RUN                   NOWRITE_PROTECT        READ_CACHE
          READAHEAD_CACHE       WRITEBACK_CACHE
          MAXIMUM_CACHED_TRANSFER_SIZE = 1
       Access:
         BuildngBA,BuildngBB,BuildngBC,BuildngBD,HOSTA1,HOSTA2
State:
          ONLINE to this controller
          Not reserved
          PREFERRED_PATH = OTHER_CONTROLLER
          Host based logging NOT specified
          Target NORMAL
        Size:             17769177 blocks
        Geometry (C/H/S): ( 5258 / 20 / 169 )
```

5. To see the connection name, operating system, controller, controller port, adapter ID address, online or offline status, and unit offset, issue the following CLI command:

   ```
   SHOW CONNECTIONS
   ```

You should see a display similar to that in Example Display 56 for each connection.

Example Display 56

```
    Connection Unit
  Name     Operating system     Controller    Port    Address     Status Offset
 HostA1   WINNT         THIS       1    634000    OLthis   0
                HOST_ID=1000-0000-C921-4B5B ADAPTER_ID=1000-0000-C921-4B5B
```

6. Click **Stop** to end the Capture Text function. Your work has been saved in the file created in step 3 in the Terminal Emulator Session, page 145.
7. Print two copies of this file for future reference. Retain one copy at each site. This hard copy is preferred because the computer or storage containing the on-line copy may not be available during an emergency.
8. Repeat this procedure, “Documenting Your Configuration,” for all subsystems in your configuration.

Configuring the Optional Entry-Level DRM Solutions

5

This chapter describes the entry-level DRM solutions and explains how to set up and configure them.

This chapter covers the following topics:

- Dual-Switch Single-Site Configuration, page 150
- Single-Switch Configuration, page 152
- Single-Fabric Configuration, page 154

Note: It is a good idea to keep a copy of this manual at both the initiator and target sites to ensure a successful and identical setup at both sites. Two copies also eliminate confusion if more than one person is configuring DRM.

Overview

Table 7 summarizes and compares the entry-level configurations.

Table 7: Comparison of Entry-Level Configurations

Configuration	Fully Redundant	Disaster Tolerant	Intersite Link (ISL)	Maximum Separation Distance between Initiator and Target	Zoning Required
Dual Switch Single Site	Yes	No	No	1000 meters	No
Single Switch	No	No	No	1000 meters	Yes
Single Fabric	No	Yes	Yes	Link technology-dependent*	Yes
*Very Long Distance GBIC = up to 100 kilometers Dense Wave Division Multiplex (DWDM) = up to 100 kilometers Asynchronous Transfer Mode (ATM) = unlimited Internet Protocol (IP) = unlimited					

Dual-Switch Single-Site Configuration

This configuration, shown in Figure 22, is designed for environments that need only local data protection in the event of local disaster or that are used as local test beds for operational DRM solutions. This solution uses only two switches, where each switch creates "a fabric in a box," instead of the multiswitch fabrics supported in full DRM solutions.

Note: The maximum separation between host and switch is 500 meters. The maximum separation between hosts is, therefore, 1000 meters or 1 kilometer.

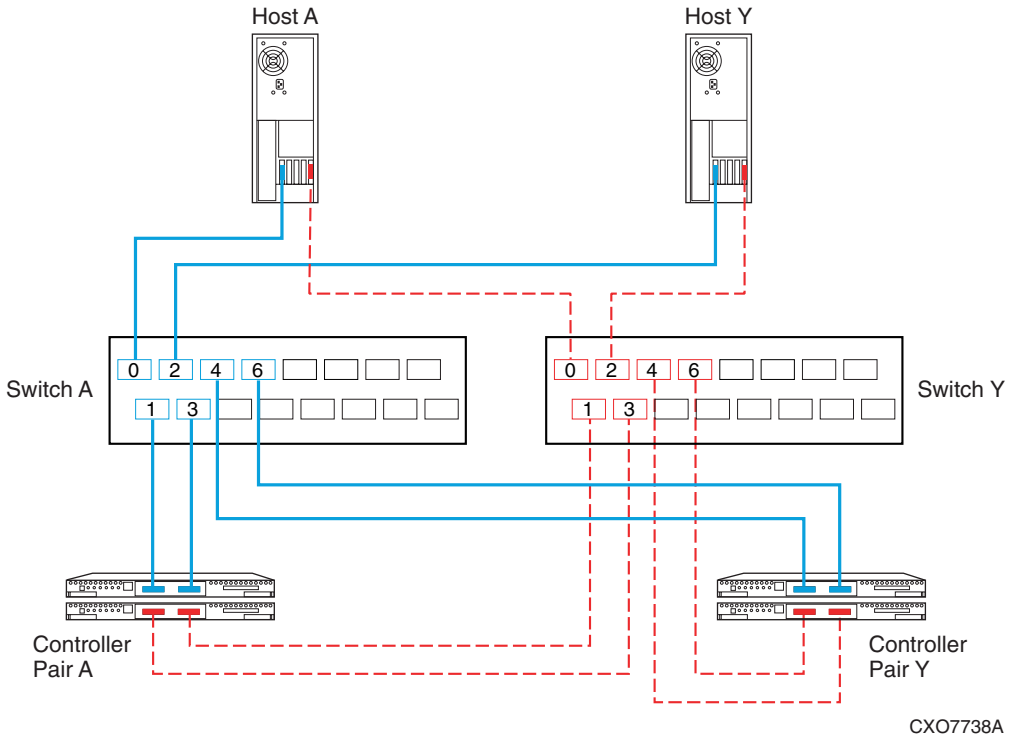


Figure 22: DRM dual-switch single-site configuration

Because of its design, a DRM dual-switch single-site configuration is limited to supporting connections equal to one switch. For example, the maximum configuration based on 8 or 16-port switches is any of the following:

- 8-port switches
  - one pair of arrays and up to four servers
- 16-port switches
  - one pair of arrays and up to twelve servers
  - two pairs of arrays and up to eight servers
  - three pairs of arrays and up to four servers

Larger port count switches are supported with limitations scaled to the increase in port count. See the DRM Release Notes for a list of supported switches. The limits on the number of servers are specified in the *HP StorageWorks SAN Design Reference Guide.*

The HSG80 Array Controller and the server host bus adapter (HBA) use only shortwave gigabit interface converters (GBICs). This means that the DRM Dual-Switch Single-Site configuration is limited to 500 meters of 50-micron or 200 meters of 62.5-micron multimode fiber optic cable between the HBA and either switch and between the controller and either switch. This limits the DRM Dual-Switch Single-Site configuration to a maximum separation of 1 kilometer, using 50-micron cable (400 meters with 62.5-micron cable), between primary and alternate servers and between primary and alternate storage arrays.

To achieve this maximum distance, HP recommends locating the two switches somewhere between the primary site and the alternate site. Both switches should be installed in separate locations with unique fiber paths between the switch and both sites. This will prevent, for example, a single backhoe from cutting both fabrics and isolating the primary and alternate sites from each other. The DRM Dual-Switch Single-Site configuration is not designed to survive large area natural disasters, like earthquakes, tornadoes, or hurricanes, due to the limited intersite distance.

Setting Up the Dual-Switch Single-Site DRM Configuration

Note: This configuration uses only multimode, 50-micron fiber optic cable and is, therefore, limited to 500 meters for any one connection.

Follow the procedures in Chapter 4 to configure a DRM solution, with the following exceptions:

1. Install all required shortwave GBICs into each of the Fibre Channel switches.
2. Make the following controller connections:
   a. Connect a fiber optic cable from port 1 of the top controller of Controller Pair A to port 1 of Fibre Channel switch A.
   b. Connect a fiber optic cable from port 2 of the top controller of Controller Pair A to port 3 of Fibre Channel switch A.
   c. Connect a fiber optic cable from port 1 of the bottom controller of Controller Pair A to port 3 of Fibre Channel switch Y.
   d. Connect a fiber optic cable from port 2 of the bottom controller of Controller Pair A to port 1 of Fibre Channel switch Y.
   e. Connect a fiber optic cable from port 1 of the top controller of Controller Pair Y to port 4 of Fibre Channel switch A.
   f. Connect a fiber optic cable from port 2 of the top controller of Controller Pair Y to port 6 of Fibre Channel switch A.
   g. Connect a fiber optic cable from port 1 of the bottom controller of Controller Pair Y to port 6 of Fibre Channel switch Y.
   h. Connect a fiber optic cable from port 2 of the bottom controller of Controller Pair Y to port 4 of Fibre Channel switch Y.

Note: You should see an illuminated green LED on the switch as soon as the cable is inserted at both ends. This verifies that there is a good connection.

3. Make the following connections between the hosts and the switches:
   a. Connect a fiber optic cable from port 0 of Fibre Channel switch A to one adapter in Host A.
   b. Connect a fiber optic cable from port 0 of Fibre Channel switch Y to the other adapter in Host A.
   c. Connect a fiber optic cable from port 2 of Fibre Channel switch A to one adapter in Host Y.
   d. Connect a fiber optic cable from port 2 of Fibre Channel switch Y to the other adapter in Host Y.
   e. Verify the connections between the hosts and the switches by issuing the following CLI command:

      ```
      SHOW CONNECTIONS
      ```

Note: You can also verify the connection by observing the illuminated green LED that flashes on the switch ports.

Disregard the procedure for connecting the external fiber links as described in Chapter 4 in the sections titled “Connect the Target Site to the External Fiber Link” and “Connect the Initiator Site to the External Fiber Link.” These procedures are not needed because the Dual-Switch Single-Site DRM solution does not accommodate longwave GBICs or other transport modes, because neither the controller nor the HBA support a single-mode long-distance connection.

Single-Switch Configuration

This configuration, illustrated in Figure 23, is designed for small, single-site entry-level tests and proof of concept demonstrations. This non-disaster-tolerant solution can also be used to produce copies of data needed for data migration or data mining. If a 16-port switch is used, then four ports are used for each fabric at each site. These four ports can support a maximum of two servers and one storage array per simulated site. Similar configurations can be built using larger port count switches. Switch zoning can be used to simulate the two logical fabrics used by DRM. For more information on zoning, refer to your switch documentation. Refer to the DRM Release Notes for a list of supported switches.

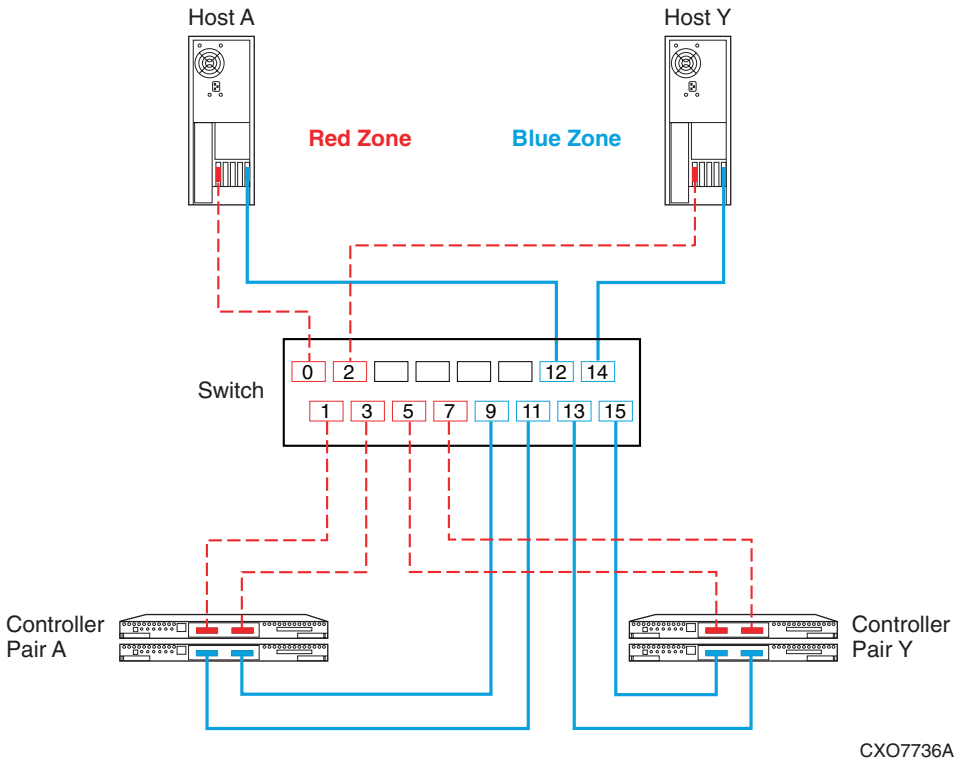


Figure 23: Single-switch DRM configuration

Setting Up the Single-Switch Configuration

Before making any connections with the fiber optic cable, create and enable the zones that simulate two fabrics. As Figure 23 shows, the Red Zone uses ports 0 through 7; the Blue Zone uses ports 8 through 15.

Note: This configuration uses only multimode, 50-micron fiber optic cable and is, therefore, limited to 500 meters for any one connection.

This procedure is a variation of the procedure provided in Chapter 4. To set up the single-switch configuration:

1. Install all required GBICs into the Fibre Channel switch, with half of the GBICs in each zone.
2. Make the following controller connections:
   a. Connect a fiber optic cable from port 1 of the top controller of Controller Pair A to port 1 of the Fibre Channel switch.
   b. Connect a fiber optic cable from port 2 of the top controller of Controller Pair A to port 3 of the Fibre Channel switch.
   c. Connect a fiber optic cable from port 1 of the bottom controller of Controller Pair A to port 11 of the Fibre Channel switch.
   d. Connect a fiber optic cable from port 2 of the bottom controller of Controller Pair A to port 9 of the Fibre Channel switch.

e. Connect a fiber optic cable from port 1 of the top controller of Controller Pair Y to port 5 of the Fibre Channel switch.

f. Connect a fiber optic cable from port 2 of the top controller of Controller Pair Y to port 7 of the Fibre Channel switch.

g. Connect a fiber optic cable from port 1 of the bottom controller of Controller Pair Y to port 15 of the Fibre Channel switch.

h. Connect a fiber optic cable from port 2 of the bottom controller of Controller Pair Y to port 13 of the Fibre Channel switch.

Note: You should see an illuminated green LED on the switch as soon as each cable is inserted at both ends. This verifies that there is a good connection.

---

3. Make the following host connections:

   a. Connect a fiber optic cable from HBA A of Host A to port 0 of the Fibre Channel switch.

   b. Connect a fiber optic cable from HBA B of Host A to port 12 of the Fibre Channel switch.

   c. Connect a fiber optic cable from HBA A of Host Y to port 2 of the Fibre Channel switch.

   d. Connect a fiber optic cable from HBA B of Host Y to port 14 of the Fibre Channel switch.

Note: Because this configuration uses only one switch, there will not be an ISL. This eliminates the procedure for connecting the external fiber links as described in Chapter 4 in the sections titled "Connect the Target Site to the External Fiber Link" and "Connect the Initiator Site to the External Fiber Link."

Single-Fabric Configuration

This configuration, illustrated in Figure 24 with 8-port switches, is designed for small, entry-level tests and proof-of-concept demonstrations where some distance is needed between the switches in the solution. Larger port count switches are also supported up to the proportional limits listed for 8-port switches. This non-disaster-tolerant solution can also be used to produce copies of data needed for data migration or data mining. Fabric zoning, if desired, is used to create two logical fabrics out of the one physical fabric. For more information on zoning, refer to your switch documentation.

Because a GBIC is used between switches, and all multimode cables are local to a switch, the ISL can be any supported transport, like single-mode fiber, dense wavelength division multiplexing (DWDM), or asynchronous transport mode (ATM). There is no distance limitation between sites.

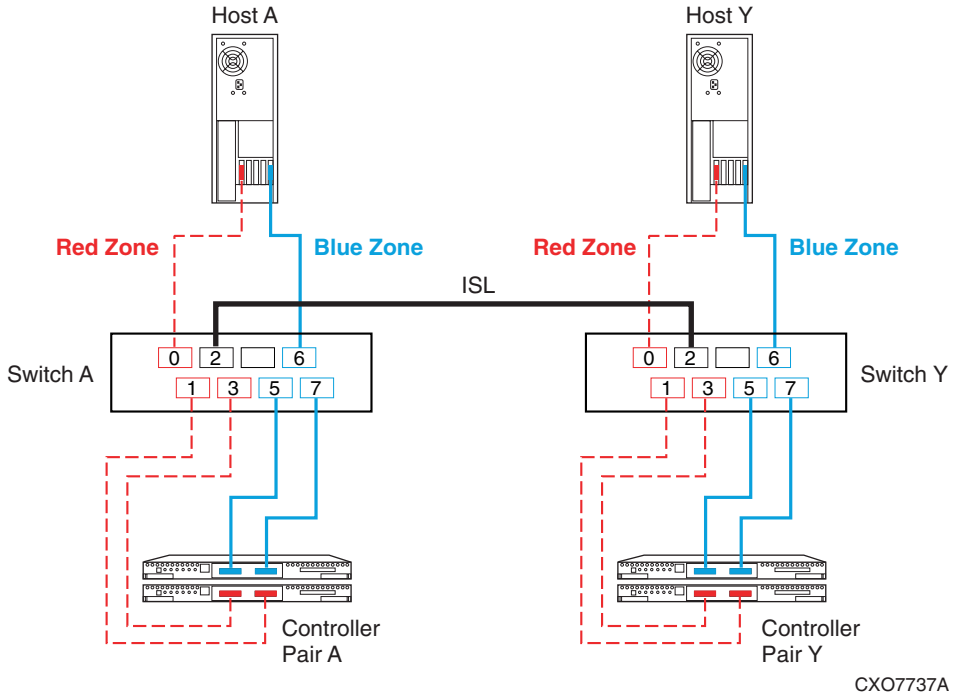


Figure 24: Dual switch with single ISL

Note: For 8-EL switches, HP recommends that the ISL connection use port 7. Port 7 is the only removable port on the 8-EL switch; the other seven are fixed, short-wave GBICs and are not suitable for ISLs.

The maximum configuration using 8 or 16 port switches is any of the following:

- 8-port switches
  - one pair of arrays, one or two ISLs, and one server
- 16-port switches
  - one pair of arrays, one or two ISLs, and up to five servers
  - two pairs of arrays, one or two ISLs, and up to three servers
  - three pairs of arrays, one or two ISLs, and one server

Larger solutions can be built using larger port count switches. See the DRM Release Notes for a list of supported switches. The limits on the number of servers are specified in the *HP StorageWorks SAN Design Reference Guide.*

The maximum distance between target and initiator is determined by the type of ISL (see Table 7).

Setting Up the Single-Fabric Configuration

Before making any connections with the fiber optic cable, create and enable the zones that simulate two fabrics. As Figure 24 shows, the Red Zone uses ports 0 through 3; the Blue Zone uses ports 4 through 7 of each switch. To create zones, refer to your switch documentation.

Note: This configuration uses multimode, 50-micron fiber optic cable on the connections from the controllers to the switches and the connections from the hosts to the switches. The ISL can use either single-mode, 9-micron fiber or multimode, 50-micron fiber, or any supported long-distance medium.

This procedure is a variation of the procedure provided in Chapter 4. To set up the single fabric configuration:

1. Install all required GBICs—except those used for the ISL—into the Fibre Channel switches, with half of the GBICs in each zone.
2. Make the following local controller connections:
   a. Connect a fiber optic cable from port 1 of the top controller of Controller Pair A to port 5 of Fibre Channel switch A.
   b. Connect a fiber optic cable from port 2 of the top controller of Controller Pair A to port 7 of Fibre Channel switch A.
   c. Connect a fiber optic cable from port 1 of the bottom controller of Controller Pair A to port 3 of Fibre Channel switch A.
   d. Connect a fiber optic cable from port 2 of the bottom controller of Controller Pair A to port 1 of Fibre Channel switch A.
3. Make the following remote controller connections:
   a. Connect a fiber optic cable from port 1 of the top controller of Controller Pair Y to port 5 of Fibre Channel switch Y.
   b. Connect a fiber optic cable from port 2 of the top controller of Controller Pair Y to port 7 of Fibre Channel switch Y.
   c. Connect a fiber optic cable from port 1 of the bottom controller of Controller Pair Y to port 3 of Fibre Channel switch Y.
   d. Connect a fiber optic cable from port 2 of the bottom controller of Controller Pair Y to port 1 of Fibre Channel switch Y.

Note: You should see an illuminated green LED on the switch as soon as the cable is inserted at both ends. This verifies that there is a good connection.

---

4. Make the following local host connections:
   a. Connect a fiber optic cable from HBA A of Host A to port 0 of Fibre Channel switch A.
   b. Connect a fiber optic cable from HBA B of Host A to port 6 of Fibre Channel switch A.

5. Make the following remote host connections:
   a. Connect a fiber optic cable from HBA A of Host Y to port 0 of Fibre Channel switch Y.
   b. Connect a fiber optic cable from HBA B of Host Y to port 6 of Fibre Channel switch Y.
6. Make the following ISL connections:
   a. Install the appropriate GBIC type (long-wave or short-wave) on each switch. They may be placed anywhere on the switches, regardless of the zoning configuration.
   b. Connect the fiber optic cable type (multimode or single-mode) to the GBICs installed in step 6a.

Configuring the Optional Advanced DRM Solutions

6

This chapter provides information on different Data Replication Manager (DRM) configurations for special circumstances.

The topics discussed in this chapter are:

- Bidirectional DRM Solution, page 159
- Stretched Cluster DRM Solution, page 160

Bidirectional DRM Solution

DRM supports active/active bidirectional solutions by using two sets of storage arrays—one set for each direction. This allows both sites to be actively processing data and backing up each other in the event that one of the two sites fails.

As shown in Figure 25, there are two servers at each site. These site-specific servers could be clustered during normal operations to provide high-availability applications. When a site failure occurs, the application that was running at the failed site is moved to the backup member of the surviving cluster, and is started using the surviving storage and the other half of the surviving cluster.

With additional servers and storage, the bidirectional DRM configuration can scale up to 20 switches in each fabric, supporting, for example, 96 servers and 8 arrays at each site. All intersite technologies—such as DRM over ATM, DRM over direct fiber, DRM over IP, and DRM over WDM—support bidirectional use of DRM.

For more information on intersite technologies, refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide*.

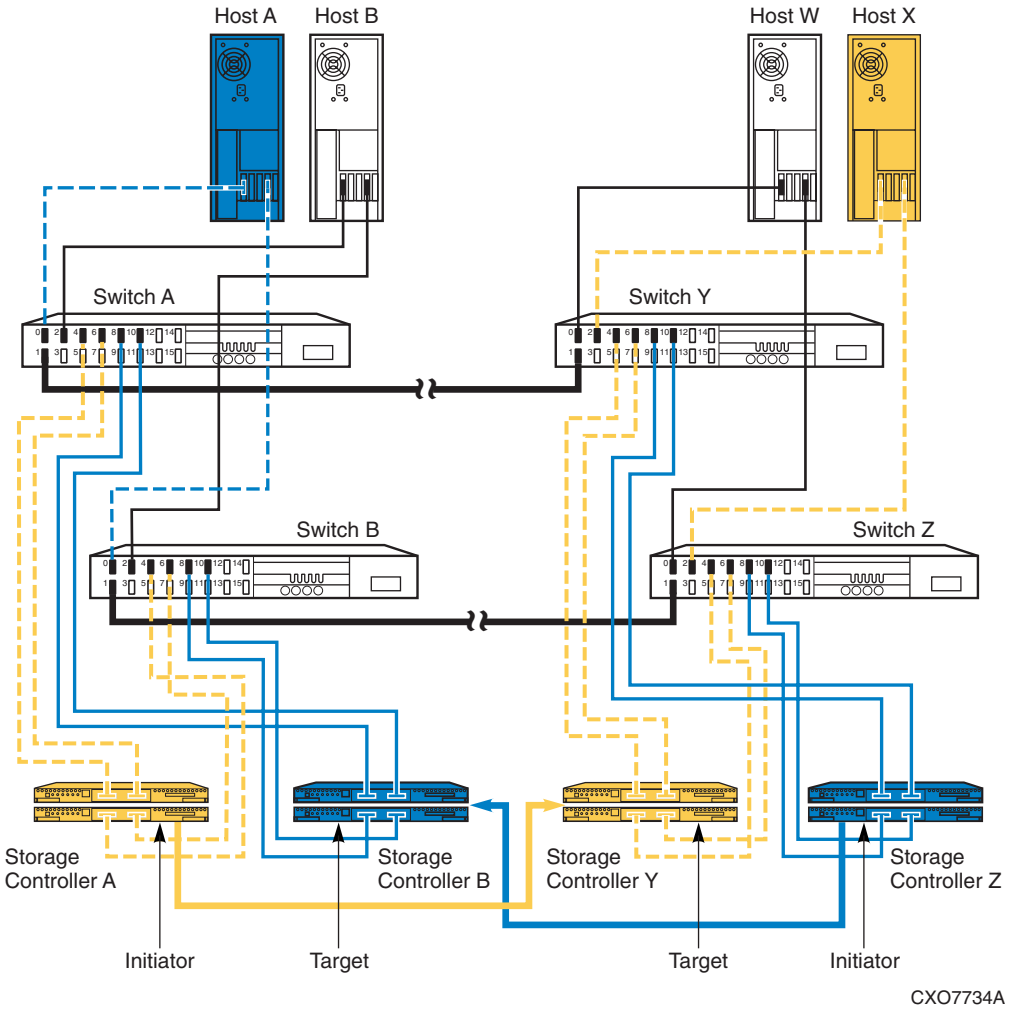


Figure 25: Bidirectional DRM configuration

Stretched Cluster DRM Solution

DRM supports Microsoft Cluster Servers (MSCS) running Windows 2000/NT. The term *stretched cluster* means that half of the cluster is at the primary site, and the other half is at the alternate site. If the primary server fails, MSCS fails over the application to the surviving server at the alternate site and resumes operations using the primary site storage.

Applications running in a stretched cluster in failover mode incur a performance penalty because of the time that it takes to read or write data across the intersite link (ISL). The performance penalty is directly proportional to the distance between the two sites—the greater the distance, the greater the penalty. However, at separation distances of up to 100 km, you should see no additional performance degradation.

For more information on stretched cluster support, go to the HP ProLiant HA/F500 website at:

http://h18000.www1.hp.com/solutions/enterprise/highavailability/microsoft/haf500/index-ma8000.html

Troubleshooting

7

This chapter shows you how to interpret information from the HSG80 controllers, the SAN switches, and the operating system to aid in troubleshooting.

The user of these troubleshooting procedures must be familiar with Data Replication Manager (DRM) procedures and CLI commands and must be proficient with the HSG80.

Refer to the *HP StorageWorks Data Replication Manager HSG80 Version 8.7P Failover/Failback Procedures Guide* for additional and more detailed troubleshooting procedures. Refer to the *HP StorageWorks HSG80 Array Controller ACS Version 8.7 Maintenance and Service Guide* for HSG80 information.

The goal of these troubleshooting procedures is to determine the cabling or connections between controllers, switches, host bus adapters (HBAs), and servers across target and initiator sites. When the actual cabling is known, it may be compared with the intended cabling to account for sources of error.

To determine the cabling, first obtain information from the controller pairs, then from the switches, and finally from the operating system.

This chapter covers the following topics:

- Preliminary Checks, page 162
- Information from the Controllers, page 162
  - Step 1: Issue a SHOW THIS Command, page 162
  - Step 2: Issue a SHOW OTHER Command, page 164
  - Step 3: Issue a SHOW CONNECTIONS Command, page 165
- Information from the Switches, page 167
  - Step 4: Issue switchShow Command from the First Switch, page 168
  - Step 5: Issue switchShow Command from the Second Switch, page 169
  - Step 6: Issue switchShow Command from the Third Switch, page 171
  - Step 7: Issue switchShow Command from the Fourth Switch, page 173
- Information from the Operating Systems, page 175
  - Step 8: Associating HBAs with Servers, page 175
- Other Troubleshooting Considerations, page 179
  - SHOW Commands, page 179
  - Zoning, page 180

— Secure Path, page 180

■ Controller Replacement in a DRM Configuration, page 181

Preliminary Checks

Before you begin the troubleshooting procedures, verify that the hardware components have power and are functioning properly. For help getting a terminal connection to the controller, refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 Installation and Configuration Guide* for your operating system. See the *HP StorageWorks HSG80 Array Controller ACS Version 8.7 Troubleshooting Reference Guide* for a checklist of common problems.

When you have determined that the hardware is working properly, issue `SHOW` commands to verify that your storage sets, units, and association sets are configured correctly. Refer to the *HP StorageWorks HSG80 ACS Solution Software Version 8.7 Installation and Configuration Guide* (for your operating system) and the *HP StorageWorks HSG80 Array Controller ACS Version 8.7 Troubleshooting Reference Guide* for more information. See the *HP StorageWorks Data Replication Manager HSG80 Version 8.7P Failover/Failback Procedures Guide* for information specific to DRM failures during failover and failback.

Information from the Controllers

Follow the steps in this section to acquire cabling information from the controllers.

Step 1: Issue a SHOW THIS Command

Telnet into the initiator-controller pair and issue a `SHOW THIS` CLI command. Table 8 shows typical output from a `SHOW THIS` command and highlights in boldface the information relevant to troubleshooting.

Table 8: SHOW THIS Command Analysis

SHOW THIS command output	What to look for	Related Commands
Controller:		
HSG80 **ZG94115534** Software **V87P**, Hardware	Make sure serial number is unique. Check the ACS version (here it is 8.7P).	Your WWIDs will be different from those shown in this example.
NODE_ID = **5000-1FE1-0007-9DD0**	Make sure the NODE_ID (WWID) is	
ALLOCATION_CLASS = 0		
SCSI_VERSION = **SCSI-3**	SCSI-3 only for OpenVMS; SCSI-2 or SCSI-3 for Tru64 UNIX, NetWare, Windows NT and Windows 2000; SCSI-2 only for AIX and Solaris.	set this scsi_version=scsi-3
Configured for **MULTIBUS_FAILOVER** with **ZG94416756**	Verify multibus failover mode. Verify that the serial number is unique.	set multibus_failover copy=this
Device Port SCSI address 7		
Time: 02-APR-2001 16:06:21	Set the time before running FRUTIL.	set this time = 02-APR-2001:16:06:00
Command Console LUN is lun **0** (NOIDENTIFIER)	SCSI-3 sets this automatically to 0.	
Host PORT_1:		
Reported PORT_ID = 5000-1FE1-0007-9DD**3**	Top controller port 1 address	
PORT_1_TOPOLOGY = **FABRIC** (fabric up)	If offline, there is no connection to host.	set this port_1_topology=fabric
Address = 2**1**0**4**13	Switch domain 1 port 4 is connected to port 1. Note that the second number in the switch port connection address is the switch domain and the fourth number is the port number on the switch.	
Host PORT_2		
Reported PORT_ID = 5000-1FE1-0007-9DD**4**	Top controller port 2 address	
PORT_2_TOPOLOGY = **FABRIC** (fabric up)	If offline, there is no connection to target.	set this port_2_topology=fabric
Address = 2**1**0**5**13	Switch domain 1 port 5 is connected to port 2.	
REMOTE_COPY = **BUILDNGA**	Alias for this pair of controllers	set this remote_copy= BUILDNGA
Cache:		
256 megabyte write cache, version 0012	256 MB (512 MB before mirroring) is minimum required for DRM	set this mirrored_cache
Cache is **GOOD*****	If cache is invalid, it needs to be flushed	clear this_invalid cache destroy_unflushed data
No unflushed data in cache		
CACHE_FLUSH_TIMER = DEFAULT (10 seconds)		
Mirrored Cache:		
256 megabyte write cache, version 0012		
Cache is GOOD		
No unflushed data in cache		
Battery:		
NOUPS		
FULLY CHARGED	If the battery is insufficiently charged, wait until it is fully charged or, if necessary, replace the battery	run FRUTIL

The WWID (NODE_ID) in Table 8 is 5000-1FE1-0007-9DD0; the four ports on the controller pair are always arranged as shown in Figure 26. The -9DD0 WWID for the controller pair dictates the -9DD1 through -9DD4 WWIDs for the ports.

Note: The WWID numbering scheme shown in Figure 26 is true only when the controllers are in multibus failover mode; it is not true for transparent mode.

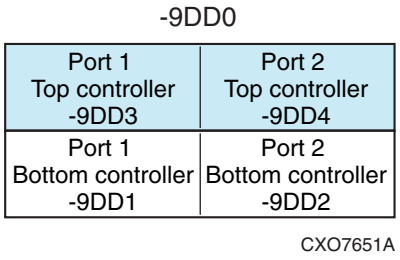


Figure 26: Controller pair World Wide IDs

Step 2: Issue a SHOW OTHER Command

Check for consistency in the other controller by issuing a `SHOW OTHER` command. Table 9 shows a typical output from the `SHOW OTHER` command and highlights the information relevant to troubleshooting.

Table 9: SHOW OTHER Command Analysis

SHOW OTHER Command Output	What to look for
Controller:	
HSG80 ZG94416756 Software **V87P**, Hardware E10	Verify ACS code version is same on both controllers.
NODE_ID = 5000-1FE1-0007-9DD0	
ALLOCATION_CLASS = 0	Allocation class may be set by OpenVMS.
SCSI_VERSION = SCSI-3	SCSI version may also be SCSI-2.
Configured for **MULTIBUS_FAILOVER** with ZG94115534	Verify that controller is in multibus failover mode.
In a dual-redundant configuration	
Device Port SCSI address 6	
Time: 02-APR-2001 16:06:21	
Command Console LUN is lun 0 (NOIDENTIFIER)	
Host PORT_1:	
Reported PORT_ID = 5000-1FE1-0007-9DD1	
PORT_1_TOPOLOGY = FABRIC (fabric up)	
Address = 2**00**4**1**3	Switch domain 0, port 4.
Host PORT_2	

Table 9: SHOW OTHER Command Analysis (Continued)

SHOW OTHER Command Output	What to look for
Reported PORT_ID = 5000-1FE1-0007-9DD2 PORT_2_TOPOLOGY = FABRIC (fabric up) Address = 2**0**0**6**13 REMOTE_COPY = BUILDNGA	Switch domain 0, port 6.
Cache: 256 megabyte write cache, version 0012 Cache is GOOD No unflushed data in cache CACHE_FLUSH_TIMER = DEFAULT (10 seconds)	
Mirrored Cache: 256 megabyte write cache, version 0012 Cache is GOOD No unflushed data in cache	
Battery: NOUPS FULLY CHARGED Expires: WARNING: UNKNOWN EXPIRATION DATE! WARNING: AN UNKNOWN NUMBER OF DEEP DISCHARGES HAVE OCCURRED!	If the battery is insufficiently charged, wait until it is fully charged or, if necessary, replace the battery. Run *FRUTIL* to set the expiration date.

From the `SHOW THIS` and `SHOW OTHER` command results, we know that there are two switches: domain 0 (from the port addresses highlighted in Table 9) and domain 1 (from the port addresses highlighted in Table 8). We also know that the storage array is connected as follows:

- Switch domain 1, ports 4 and 5 are cabled to the top controller (port addresses 2**1**0**4**13 and 2**1**0**5**13 in Table 8)
- Switch domain 0, ports 4 and 6 are cabled to the bottom controller (port addresses 2**0**0**4**13 and 2**0**0**6**13 in Table 9)

Step 3: Issue a SHOW CONNECTIONS Command

Issue a `SHOW CONNECTIONS` command to show which connections the controller can see. Table 10 shows a typical output from the `SHOW CONNECTIONS` command and highlights the information relevant to troubleshooting.

Table 10: SHOW CONNECTIONS Command Analysis

SHOW CONNECTIONS Command Output	Comments
Connection Unit Name Operating system Controller Port Address Status Offset **!NEWCON66 WINNT** THIS 1 200013 OL this 0 HOST_ID=1000-0000-C920-C9E1 ADAPTER_ID=1000-0000-C920-**C9E1**	Choose a meaningful name; example: rename !newcon66 hostA_1. Set to proper operating system type; example: set !newcon66 operating_system=SUN.
!NEWCON67 WINNT OTHER 1 200013 OL other 0 HOST_ID=1000-0000-C920-C9F0 ADAPTER_ID=1000-0000-C920-**C9F0**	
!NEWCON68 WINNT THIS 1 200013 **OL this** 0 HOST_ID=1000-0000-C921-F21A ADAPTER_ID=1000-0000-C921-**F21A**	Online to this controller.
!NEWCON69 WINNT OTHER 1 200013 OL other 0 HOST_ID=1000-0000-C921-F251 ADAPTER_ID=**1000-0000-C921-F251**	WWID of HBA.
BUILDNGBA PPRC_TARGET THIS **2** 200513 **OL** this 0 HOST_ID=5000-1FE1-0007-9DE0 ADAPTER_ID=5000-1FE1-0007-9DE4	BUILDNGBA and BUILDNGBB must be online to the initiator for remote copy sets to work. Example: add remote rcs199 d199 buildngb\d199.
BUILDNGBB PPRC_TARGET OTHER **2** 210E13 **OL** other 0 HOST_ID=5000-1FE1-0007-9DE0 ADAPTER_ID=5000-1FE1-0007-9DE2	
BUILDNGBC PPRC_INITIATOR THIS **2** 200513 offline 0 HOST_ID=5000-1FE1-0007-9DE0 ADAPTER_ID=5000-1FE1-0007-9DE4	
BUILDNGBD PPRC_INITIATOR OTHER **2** 200513 offline 0 HOST_ID=5000-1FE1-0007-9DE0 ADAPTER_ID=5000-1FE1-0007-9DE2	

Notice the port usage for each connection. In multiple-bus failover mode with remote copy enabled (that is, a DRM configuration), port 1 on each controller is connected only to HBAs. Port 2 on each controller is connected only to other controllers. Ports 1 and 2 are reserved ports for DRM configurations.

Make a note of each adapter's WWID. The controller adds a new connection entry when any of the following keys change:

- Host WWID
- Adapter WWID
- Controller host port number
- Controller WWID

There will be four connections through port 2, labeled A, B, C, and D. In the example in Table 10, they are BUILDNGBA, BUILDNGBB, BUILDNGBC, and BUILDNGBD. In most cases, only two of these connections are online: A and B at the initiator site; C and D at the target site. A and B are used to write to the target site, and C and D receive write requests from the initiator site. Thus, initiator A writes to target C and initiator B writes to target D.

We now know that we are online to four HBAs whose adapter IDs end in -C9E1, -C9F0, -F21A, and -F251. We also know that unit address 200013 is switch domain 0, port 0. There appear to be two different adapters cabled to the same switch: -F251 and -C9E1, both to port 0. That cannot be the case, because there cannot be two switch domain 0s on the same fabric. We actually have two switch 0s and two switch 1s. The best way to confirm this is to Telnet to the switches and issue the `switchShow` command.

Information from the Switches

Note: These procedures are specific to B-series Fibre Channel switches. Refer to your vendor switch documentation for information on accessing and using commands for your particular switch family and performing similar switch tasks. See the DRM Release Notes for a list of supported switch families and switch firmware versions.

Telnet into a switch and check its firmware version by issuing the version command at the switch prompt. The command and its output will be similar to that shown in Table 11.

Table 11: Switch Version Command

```
sw11:admin>  version
Kernal:  5.3.1
Fabric OS:   v2.1.7
Made on: Wed May 24 14:47:36 PDT 2000
Flash:  Wed May 24 14:48:05 PDT 2000
BootProm  Thu Jun 17 15:20:39 PDT 1999
```

Caution: Switches with incompatible firmware will cause the fabric to segment. Switches in the same fabric with the same domain number will also cause the fabric to segment. To change the domain number, issue the `CONFIGURE SWITCH` command.

Step 4: Issue switchShow Command from the First Switch

Issue a SWITCHSHOW command at the switch prompt to see the port connections:

```
sw11:admin>  switchShow
```

Table 12 shows typical output from the SWITCHSHOW command and highlights the information relevant to troubleshooting.

Table 12: First switchShow Command Output

Command Output	Comments
switchName: **sw11**	Name of the switch
switchType: 2.4	
switchState: online	
switchRole: Principal	
switchDomain: **1**	Domain
switchId: fffc41	
switchWwn: **10:00:00:60:69:10:47:69**	WWID
port 0: sw Online F-Port **10:00**:00:00:c9:20:**c9:f0**	WWIDs that start with 10:00 are HBAs.
port 1: -- No_Module	
port 2: -- No_Module	
port 3: -- No_Module	
port 4: -- **No_Light**	Check for a bad GBIC or cable.
port 5: -- No_Module	
port 6: -- No_Module	
port 7: -- No_Module	
port 8: -- No_Module	
port 9: -- No_Module	
port 10: -- No_Module	
port 11: -- No_Module	
port 12: -- No_Module	
port 13: sw Online F-Port 50:00:1f:00:07:20:**9d:e1**	Cabled to port 1 of the bottom controller.
port 14: sw Online F-Port 50:00:1f:00:07:20:**9d:e2**	Cabled to port 2 of the bottom controller.
port 15: sw Online **E-Port**10:00:00:60:69:00:54:65 "sw12" (downstream)	ISL—always on E-Port.

Note: WWIDs that start with 10:00 or 20:00 are HBAs. WWIDs that start with 50:00 are controllers or controller ports. WWIDs that start with 60:00 are LUNs.

From the SWITCHSHOW command output, we know that there is an ISL from the switch named sw11 to a switch named sw12 (port 15). Figure 27 is a picture of the cabling information we have gathered so far. It is drawn from Table 12, which shows that:

- Port 0 of sw11 (where we issued the SWITCHSHOW command) is cabled to the HBA whose WWID ends in -C9F0.
- Port 13 of sw11 is cabled to port 1 of the bottom controller.
- Port 14 of sw11 is cabled to port 2 of the bottom controller.
- Port 15 of sw11 is cabled via an ISL to sw12.

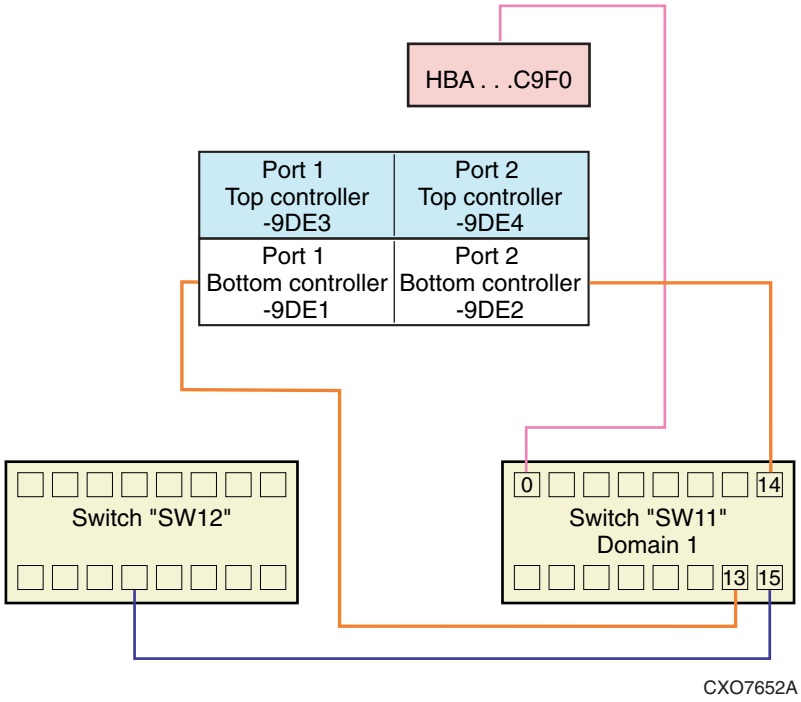


Figure 27: First cabling diagram

Step 5: Issue switchShow Command from the Second Switch

Telnet into another switch and issue a SWITCHSHOW command at the switch prompt to acquire the port connection information:

```
sw13:admin>  switchShow
```

Table 13 shows typical output from the SWITCHSHOW command.

Table 13: Second switchShow Command Output

switchName: **sw13**
switchType: 2.4
switchState: online
switchRole: Subordinate
switchDomain: **1**
switchId: fffc41
switchWwn: 10:00:00:60:69:00:51:5a
port 0: sw Online F-Port 10:00:00:00:c9:21:**f2:1a**
port 1: -- No_Module
port 2: -- No_Module
port 3: -- No_Module
port 4: -- sw Online F-Port 50:00:1f:e1:00:07:**9d:d3**
port 5: -- sw Online F-Port 50:00:1f:e1:00:07:**9d:d4**
port 6: -- sw Online **E-Port** 10:00:00:60:69:00:57:0a "**sw14**" (upstream)
port 7: -- No_Module
port 8: -- No_Module
port 9: -- No_Module
port 10: -- No_Module
port 11: -- No_Module
port 12: -- No_Module
port 13: -- No_Module
port 14: -- No_Module
port 15: -- No_Module
value = 16 = 0x10

Note: This switch is named sw13, which also has a domain of 1. We recommend that each switch have a unique domain within the fabric. We recommend unique names even across fabrics.

Figure 28 is a picture of the cabling information we have gathered so far. The cabling information added to Figure 28 is drawn from Table 13, which shows that:

- Port 0 of sw13 (where we issued the `SWITCHSHOW` command) is cabled to the HBA whose WWID ends in -F21A.
- Port 4 of sw13 is cabled to port 1 of the top controller at the same site.
- Port 5 of sw13 is cabled to port 2 of the top controller at the same site.
- Port 6 of sw13 is cabled via an ISL to sw14.

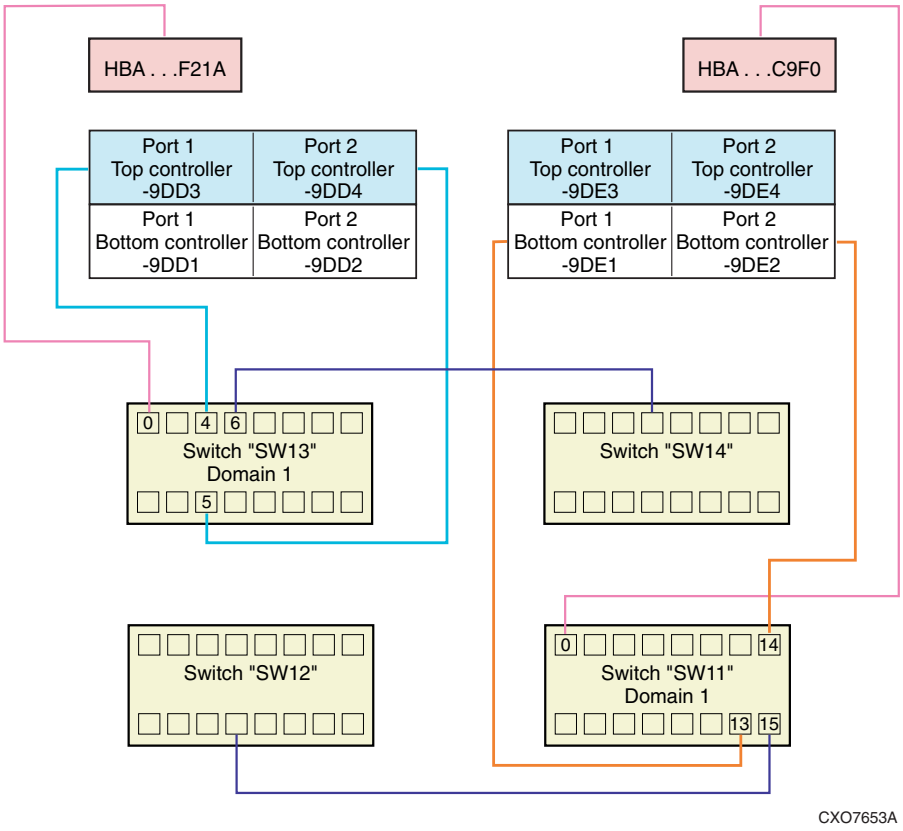


Figure 28: Second cabling diagram

Step 6: Issue switchShow Command from the Third Switch

Telnet into the third switch and issue a `SWITCHSHOW` command at the switch prompt to acquire the port connection information:

```
sw12:admin>  switchShow
```

Table 14 shows typical output from the `SWITCHSHOW` command.

Table 14: Third switchShow Command Output

switchName: **sw12**
switchType: 2.4
switchState: Online
switchRole: Principal
switchDomain: 0
switchId: fffc40
switchWwn: 10:00:00:60:69:00:54:65
port 0: sw Online F-Port 10:00:00:00:c9:21:**f2:51**
port 1: -- No_Module
port 2: -- No_Module
port 3: -- No_Module
port 4: -- sw Online F-Port 50:00:1f:e1:00:07:**9d:d1**
port 5: -- No_Module
port 6: -- sw Online F-Port 50:00:1f:e1:00:07:**9d:d2**
port 7: -- sw Online E-Port 10:00:00:60:69:10:47:69 "**sw11**" (downstream)
port 8: -- No_Card
port 9: -- No_Card
port 10: -- No_Card
port 11: -- No_Card
port 12: -- No_Card
port 13: -- No_Card
port 14: -- No_Card
port 15: -- No_Card
value = 16 = 0x10

Figure 29 is the cabling diagram with the port connections from the sw12 switch added. The additional cabling is drawn from information highlighted in Table 14, which shows that:

- Port 0 of sw12 is cabled to the HBA whose WWID ends in -F251.
- Port 4 of sw12 is cabled to port 1 of the bottom controller at the same site.
- Port 6 of sw12 is cabled to port 2 of the bottom controller at the same site.
- Port 7 of sw12 is cabled via an ISL to sw11 (compare with port 15 of sw11 in Table 12).

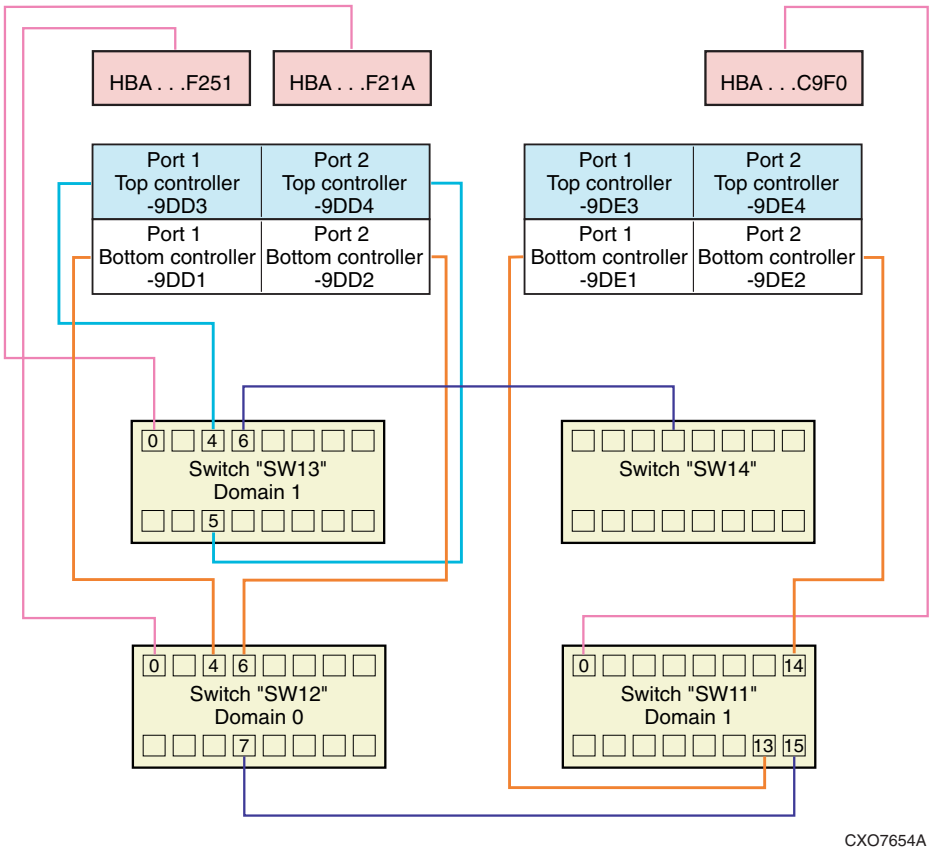


Figure 29: Third cabling diagram

Step 7: Issue switchShow Command from the Fourth Switch

Telnet into the fourth and final switch and issue a `SWITCHSHOW` command at the switch prompt to acquire the port connection information:

```
sw14:admin>  switchShow
```

Table 15 shows typical output from the `SWITCHSHOW` command.

Table 15: Fourth switchShow Command Output

switchName: **sw14**
switchType: 2.4
switchState: Online
switchRole: Principal
switchDomain: 0
switchId: fffc40
switchWwn: 10:00:00:60:69:00:57:0a
port 0: sw Online F-Port 10:00:00:00:c9:20:**c9:e1**
port 1: -- No_Module
port 2: -- No_Module
port 3: -- No_Module
port 4: -- sw Online F-Port 50:00:1f:e1:00:07:**9d:e3**
port 5: -- sw Online F-Port 50:00:1f:e1:00:07:**9d:e4**
port 6: -- sw Online E-Port 10:00:00:60:69:00:51:5a "**sw13**" (downstream)
port 7: -- No_Module
port 8: -- No_Module
port 9: -- No_Module
port 10: -- No_Module
port 11: -- No_Module
port 12: -- No_Module
port 13: -- No_Module
port 14: -- No_Module
port 15: -- No_Module

Figure 30 is the cabling diagram with the port connections from the sw14 switch added. The additional cabling is drawn from information highlighted in Table 15, which shows the cabling for all four switches:

- Port 0 of sw14 is cabled to the HBA whose WWID ends in -C9E1.
- Port 4 of sw14 is cabled to port 1 of the top controller at the same site.
- Port 5 of sw14 is cabled to port 2 of the top controller at the same site.
- Port 6 of sw14 is cabled via ISL to port 6 of sw13 (compare with port 6 of sw13 in Table 13).

Information from the Operating Systems

Figure 30 shows both fabrics (two sets of switches that communicate), but we do not yet know which HBAs go to which servers.

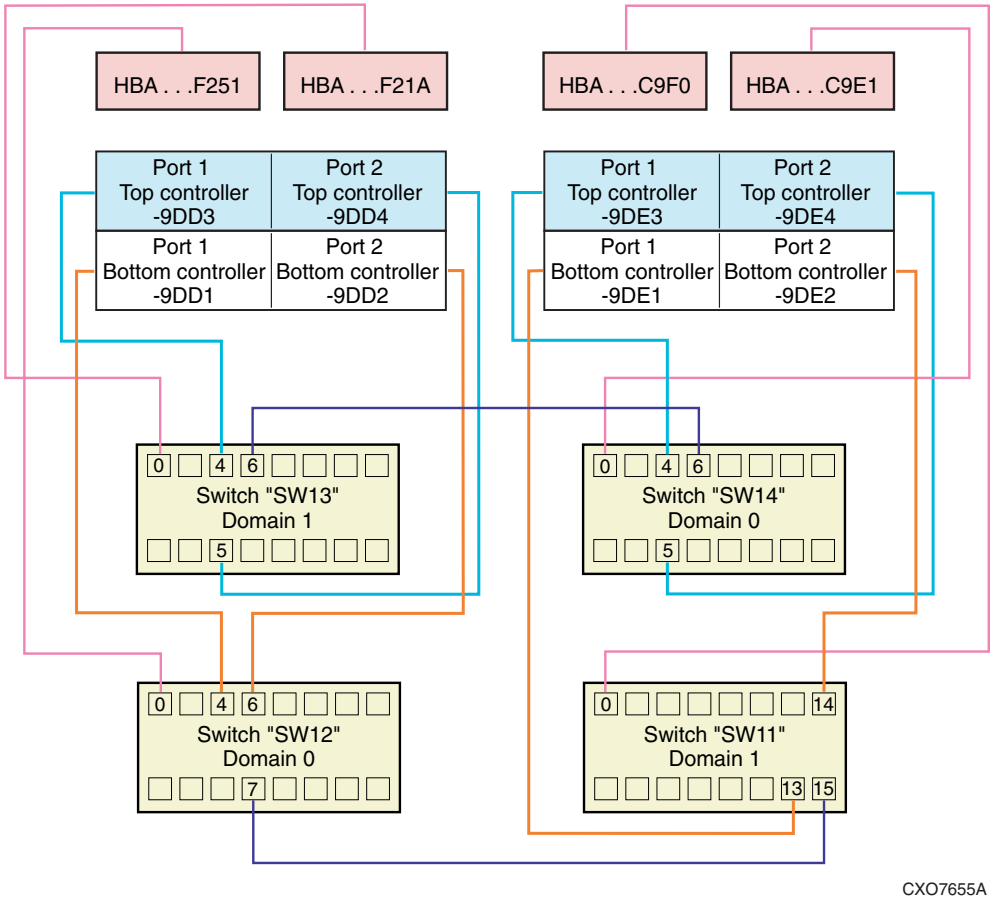


Figure 30: Fourth cabling diagram

Step 8: Associating HBAs with Servers

Our ability to associate HBAs with servers (without removing the adapter from the server and reading the label) depends on operating system and platform type. The following sections provide procedures for determining the server WWIDs for each operating system.

HP OpenVMS

Shut down the system and use the console WWID manager to issue the following commands:

```
>>>  Set mode diag
POO>>>  wwidmgr  -adapter  kgpsa0
POO>>>  wwidmgr  -adapter  kgpsa1
```

Repeat for each server.

HP Tru64 UNIX

Issue the following command at the system prompt:

```
#uerf  -R  -r  300|more
```

This shows what the system found during boot; it includes the WWID of the HBAs and the revision level of the emx driver.

Repeat for each server.

HP-UX

Issue the following command to get a display of HBAs:

```
ioscan -fn
```

The output from this command will be similar to:

```
Class I  H/W Path Driver S/W State H/W Type   Description

fc    0  0/2/0/0  td     CLAIMED   INTERFACE  HP Tachyon TL/TS Fibre Channel Mass Storage
Adapter
```

Issue the following command to get a display of an HBA's WWN:

```
/opt/fcms/bin/fcmsutil /dev/tdI
```

where I is the instance number.

Using the I value obtained from the ioscan, issue the commands:

```
/opt/fcms/bin/fcmsutil /dev/td0

N_Port Port World Wide Name = 0x50060b00000a354e
```

Repeat for each HBA instance.

IBM AIX

Issue the following command from a command console prompt to obtain WWIDs for all Cambex adapters:

```
lsdev  -Cc adapter
```

This command produces output similar to the following:

```
scsix Available 20-58 Cambex Fibre Channel I/O Controller
```

where *x* is a numeric value assigned by the operating system.

Using the x value obtained from the previous command, issue the command:

```
lscfg  -vl scsix
```

where *x* is a numeric value assigned by the operating system. The value following Network Address is the WWID.

Now that we can determine which HBAs are in each host, there is enough information to complete the configuration diagram. Figure 31 shows the complete configuration.

Microsoft Windows NT and Windows 2000

Execute the following procedure:

1. Shut down the server.
2. Boot the server from a bootable DOS diskette.
3. Insert the KGPSA diskette shipped with the adapter for Intel part AK-RF2LC-CA.
4. Issue the following DOS commands:

```
A:\cd I386
A:\1p6dutil
```

5. Select **option 6** (**Show Host adapters info**).
6. Select Host Adapter (1 or 2).
7. Write down its WWID.
8. Exit the menu by selecting 0.
9. Exit the program by selecting menu item 7.

Repeat for each server.

Novell NetWare

To obtain WWIDs for NetWare systems, you must read them directly from the adapters or from your notes taken during installation.

Sun Solaris

Issue the following command at the system prompt:

```
#more  /var/adm/messages
```

Look for the driver name like *fcaw*. It lists the adapter WWIDs, which start with 10:00 or 20:00.

Repeat for each server.

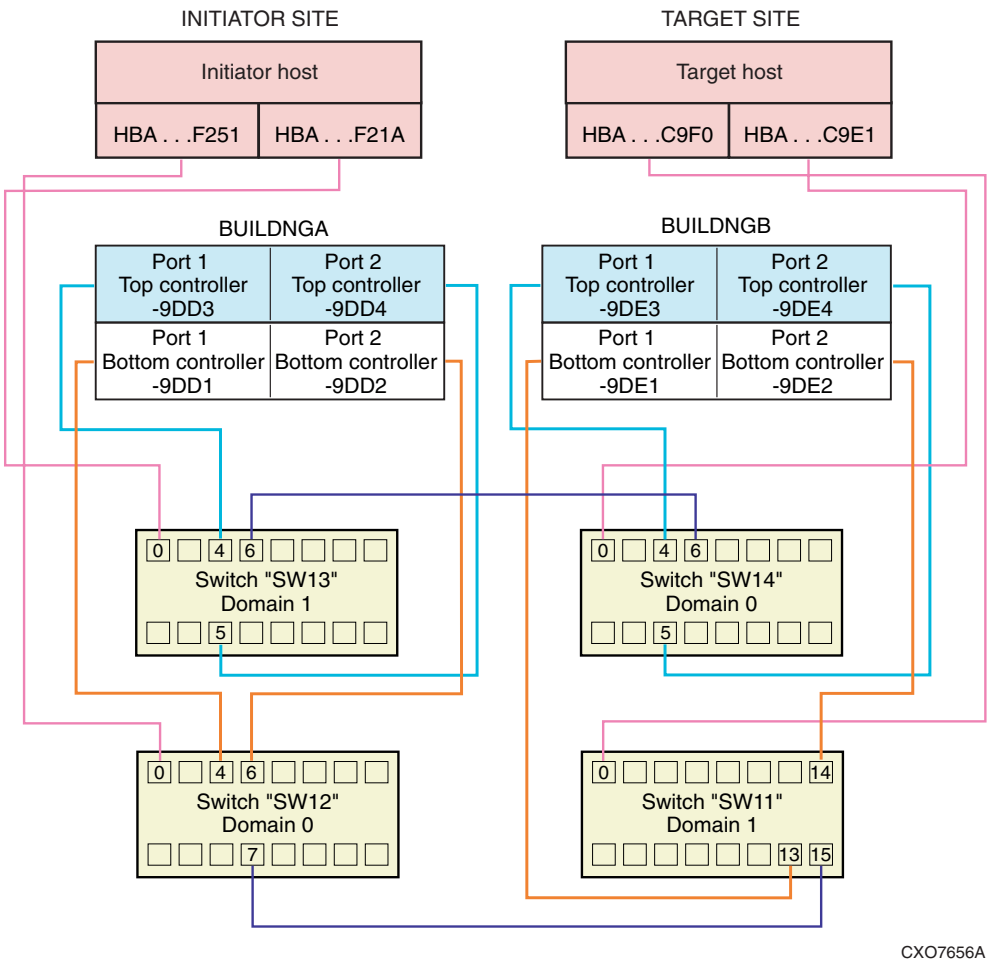


Figure 31: Final configuration

Verify that the configuration in Figure 31 is the design that was intended and that there are two fabrics. Verify that it is configured for no single point of failure.

Other Troubleshooting Considerations

SHOW commands, zoning, and Secure Path may also assist in troubleshooting.

SHOW Commands

Information useful for troubleshooting can be acquired by issuing various SHOW commands. See Appendix A for a list of SHOW commands used in troubleshooting. Two particularly useful commands are SHOW UNITS FULL and SHOW REMOTE FULL.

SHOW UNITS FULL

At the initiator controller, issue the SHOW UNITS FULL command. Table 16 shows a typical output.

Table 16: SHOW UNITS FULL Command Output

LUN Uses Used by	

D1 DISK10000	
LUN ID: 6000-1FE1-0008-0A50-0009-0510-3520-0001	
NOIDENTIFIER	
Switches:	
RUN NOWRITE_PROTECT READ_CACHE	
READAHEAD_CACHE WRITEBACK_CACHE	
MAX_READ_CACHED_TRANSFER_SIZE = 32	
MAX_WRITE_CACHED_TRANSFER_SIZE = 32	
Access:	
HOSTA_1, HOSTA_2, BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD	Check for proper access (that is, hosts and target controllers).
State:	
ONLINE to this controller	Verify that it is online.
Not reserved	If Tru64, watch for persistent reserve.
NOPREFERRED_PATH	
Size: 17769177 blocks	
Geometry (C/H/S): (5258 / 20 / 169)	

SHOW REMOTE FULL

At the initiator controller, issue the SHOW REMOTE FULL command. Table 17 shows a typical output.

Table 17: SHOW REMOTE FULL Command Output

Name Uses Used by --- RCS1 remote copy D1 A1 Reported LUN ID: 6000-1FE1-0009-1D70-0009-9421-3547-0176 Switches: OPERATION_MODE = SYNCHRONOUS ERROR_MODE = **FAILSAFE** FAILOVER_MODE = MANUAL OUTSTANDING_IOS = 20 Initiator (BUILDNGA\D1) state: ONLINE to this controller Not reserved Target state: **BUILDNGB\D1 is NORMAL**	If in failsafe mode, units can become failsafe locked. Verify that the remote copy set has a target.

Zoning

Improper zoning can prevent the proper access to controllers and hosts. Refer to your switch documentation for information on zoning and to Chapter 6, "Configuring the Optional Advanced DRM Solutions," in this guide for information on zoning for a DRM configuration.

Secure Path

If the same unit shows up twice in AIX, Solaris, NetWare, Windows NT, or Windows 2000, or does not show up at all, then Secure Path is not working properly. Refer to the *HP StorageWorks Secure Path Installation and Reference Guide* for your operating system.

Note: Secure Path does not apply to OpenVMS or Tru64 UNIX because they both have built-in multibus driver support.

Controller Replacement in a DRM Configuration

When a failed controller running ACS V8.7P needs to be replaced, follow the supported procedures in the *HP StorageWorks HSG60 and HSG80 Controller and HSx80 Cache Module Replacement Procedures for Array Controller Software V8.7x-x Release Notes*. This document can be obtained at:

http://h18006.www1.hp.com/products/sanworks/drm/relatedinfo.html

It is important to note that these procedures specify a new controller from the factory or a newly initialized (purged of an old configuration) controller. Using a factory-fresh or newly initialized (configuration-free) controller is particularly important when your configuration is set up for DRM. Failure to use a newly initialized controller causes cache corruption on the replacement controller mirrored cache.

Zoning in the Storage Area Network

8

This chapter describes Data Replication Manager (DRM) concepts and variations for alternative DRM configurations. These descriptions include cascaded switches, multiple intersite links (ISLs), dual-switch single-site DRM solutions, and switch zoning.

The topics in this chapter are:

- Switch Zoning, page 184
- Planning Considerations for Homogeneous and Heterogeneous Configurations That Require Zoning, page 184
- Zoning Hosts and HSG80 Subsystems Between Sites, page 185
  - More than 96 Host Connections, page 184
- Zoning a DRM Configuration, page 185
  - DRM Homogeneous Configuration, page 185
  - DRM Heterogeneous Configuration, page 197
- Zoning to Allow Host Access Between Sites, page 208

Switch Zoning

The Fibre Channel switch zoning feature provides a means to control storage area network (SAN) access at the node port level. Zoning can be used to separate one physical fabric into many virtual fabrics consisting of selected server and storage ports. This capability allows you to:

- Set up barriers between different operating environments
- Deploy logical fabric subsets by creating defined user groups
- Create separate test and maintenance areas within the fabric
- Flexibly manage a SAN while meeting the different objectives of closed user groups

With B-series switches, you can display a list of switch commands by typing `help` and `zoneHelp` at the switch prompt.

For more information on when to use switch zoning, refer to the *HP StorageWorks SAN Design Guide*. For additional information on switch zoning, refer to your particular switch documentation.

Planning Considerations for Homogeneous and Heterogeneous Configurations That Require Zoning

Planning is an essential part of the zoning process. The following sections provide guidelines and instructions for zoning your DRM solution.

Note: The examples in this section are based on B-series switches. Consult the appropriate documentation if using C- or M-series switches.

More than 96 Host Connections

A host connection is a data path from one host bus adapter (HBA) to one active controller host port, even if the host connection uses storage units on that storage system.

The HSG80 controller has a limit of 96 host connections. When a 97th connection is attempted, the connection name capacity of HSG80 controllers is exceeded. This can result in a controller fatal error.

In DRM mode, two host ports are active. One server with two HBAs has two data paths, one for each HBA. Each HBA on the fabric creates one connection per controller pair. Four connections are also created for initiator-controller-to-target- controller communication.

Switch zoning must be used to prevent more than 96 host connections to a single storage system. This allows more servers to be attached to the SAN to use other storage systems.

Zoning Hosts and HSG80 Subsystems Between Sites

In a DRM configuration, the initiator hosts are zoned so that they do not have access to the target controllers; the target hosts are zoned so that they do not have access to the initiator controllers.

There are circumstances, however, when the hosts at one site do require access to HSG80 controller pairs at both sites. This could occur when you are running scripts, OpenVMS host-based shadowing, or stretch clusters. If that is the case, go to the section titled "Zoning to Allow Host Access Between Sites," on page 208.

Zoning a DRM Configuration

This section provides zoning examples for both homogeneous and heterogeneous configurations.

DRM Homogeneous Configuration

The Fibre Channel fabric can be customized for zoning in numerous ways. The DRM uses for zoning include:

- Creating fabric functional areas by separating test or maintenance areas from production areas
- Designating closed user groups by including certain zone devices for exclusive use by zone members
- Simplifying resource utilization by logically consolidating equipment for convenience
- Facilitating time-sensitive functions by creating a temporary zone to back up a set of devices that are members of other zones
- Securing fabric areas by providing another level of software security to control port level access
- Separating operating system types and applications to control access to resources

This section provides examples of zoning a DRM configuration. The examples begin with the configuration of a DRM homogeneous environment. Additional examples illustrate creating a DRM heterogeneous environment from the homogeneous environment. The examples are from a Telnet session on a Fibre Channel storage switch that is case sensitive. Other switches may not be case sensitive.

Figure 32 shows a simplified DRM configuration that consists of six zones. For this example, the zones are designated Green Zone_Top and Green Zone_Bottom for the initiator site; Blue Zone_Top and Blue Zone_Bottom for the target site; and Red Zone_Top and Red Zone_Bottom, which contain the remote copy sets or paths.

Note: Zones are given color names in this document only as examples. You should choose names that are meaningful for your environment.

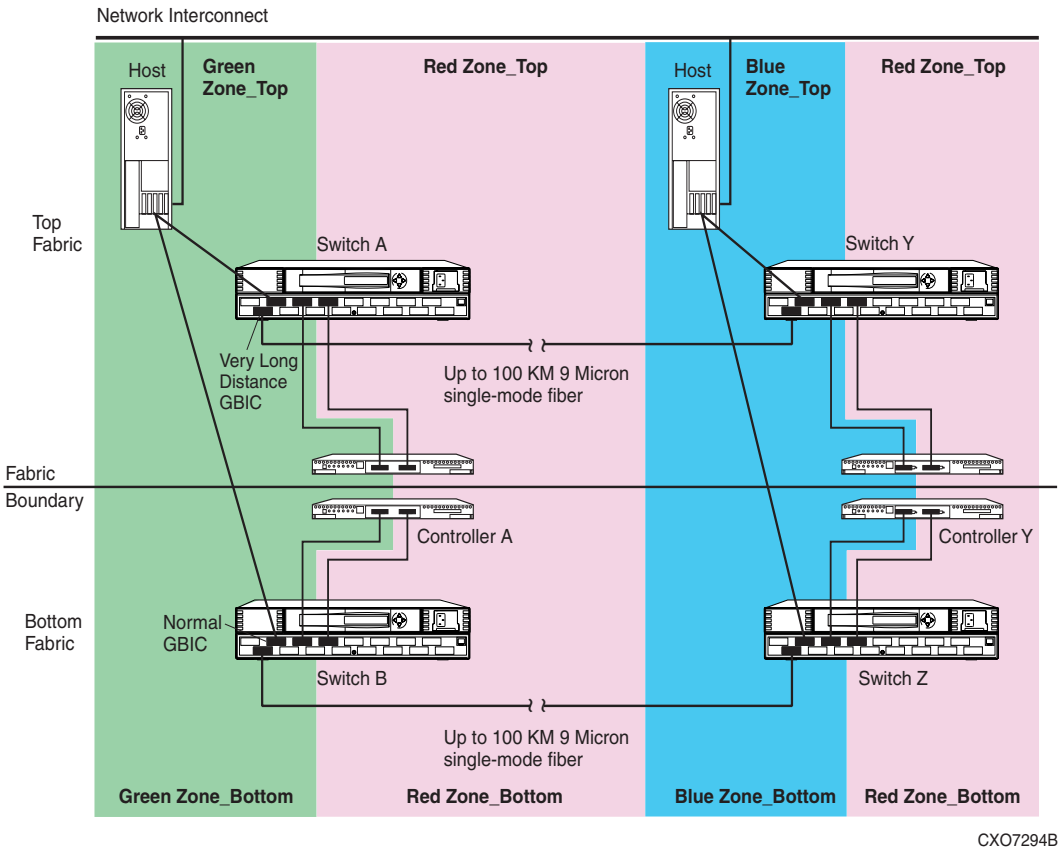


Figure 32: Zoning in a DRM homogeneous environment

HP suggests that you use Table 18, the zoning input form, to capture and track the required device and command information. The form supports two paths, two switches, and a maximum of 16 entries per switch. Copy and use a separate form to track information for each zone (such as Green Zone_Top, Blue Zone_Top, Red Zone_Top, and so on). Organize alias name, function, and site data by either World Wide ID (WWID) number or Port ID number.

Table 18: Blank zoning input form template

Zoning Configuration Name =

Zone Name= **Switch Name=** **Path=**

WWID #	Domain ID #	Port #	Alias Name	Function	Site

Zoning Configuration Name =

Zone Name= **Switch Name=** **Path=**

WWID #	Domain ID #	Port #	Alias Name	Function	Site

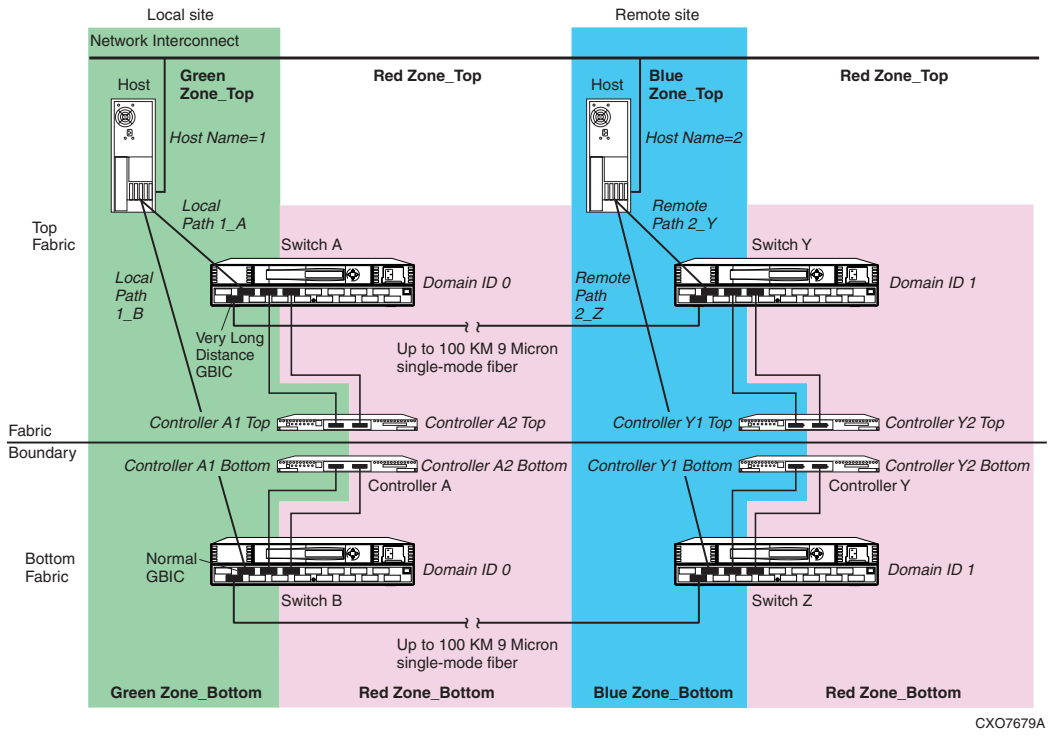


Figure 33: Zoning a DRM example

Figure 33 shows a zoned example for a Data Replication Manager configuration. The steps required to produce this zoning configuration are on the following pages. Because multiple configurations can be created and saved, the one currently in use is known as the *effective configuration*. The process to create and save an effective configuration that ensures the switches are enabled after reboot or shutdown, includes the following:

1. Begin by zoning the top fabric initiator site (designated in the example as Green Zone_Top).
2. Zone the top fabric target site (designated as Blue Zone_Top).
3. Zone the remote copy sets or paths for the top fabric (designated as Red Zone_Top).
4. Zone the three zones for the bottom fabric.

The next three examples illustrate these zoning practices.

Example: Zoning Green Zone_Top and Green Zone_Bottom

Table 19, the Green Zone_Top and Green Zone_Bottom input form, is created from a blank template (Table 18) and is added to throughout this example.

Table 19: Green Zone_Top and Green Zone_Bottom input form

Zoning Configuration Name=Top_Fabric

Zone Name=Green Zone_Top **Switch Name=Switch A** **Path=A**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	0	1	—	E-Port	Local
	0	2	Host 1_A	Host	Local
	0	4	Controller A1_top	Controller	Local

Zoning Configuration Name=Bottom_Fabric

Zone Name=Green Zone_Bottom **Switch Name=Switch B** **Path=B**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	0	1	—	E-Port	Local
	0	2	Host 1_B	Host	Local
	0	4	Controller A1_bottom	Controller	Local

Figure 33 shows zoning using the Domain ID number and the Port number, rather than the WWID number. The WWID could also have been used. A general rule is that if you are changing connections within DRM, use the WWID for zoning.

1. Identify and write down the Domain ID of each switch. To get this information, use the `switchShow` command from each switch in a Telnet session or from the front console of each switch. The example in Figure 33 shows that switches A and B both have a Domain ID of 0.

   After logging this information on a blank template form, give it the zone name "Green Zone_Top." On this form, list the Green Zone in two blocks, one for switch A in Green Zone_Top, and one for switch B in Green Zone_Bottom (see Table 19).

2. Log the ports that connect to the hosts and E-Ports.

   Figure 33 shows that "Host 1" is the host name and that there are two connections from Host 1 to the switches. Host 1 path 1_A is connected to port 2 of switch A, and Host 1 path 1_B is connected to port 2 of switch B. The E-Port is located in port 1 on both switches A and B.

3. List the controller connections for the top and bottom fabrics.

   From the example in Figure 33, the controller pair is listed as Controller A1_top (top controller, port 1), and Controller A1_bottom (bottom controller port 1). Switch A port 4 connects to Controller A1_top in the top fabric. Switch B port 4 connects to Controller A1_bottom in the bottom fabric.

4. Open a Telnet session to switch A.

5. Create the alias names in the zone. The naming convention in the example refers to Host 1_A as the host name and path for the connection to port 2 of switch A. The command for this alias is:

   ```
   aliCreate "Host 1_A", "0,2"
   ```

   This means that an alias is generated named "Host 1_A" with switch domain 0 and port number 2.

Note: Be sure to issue all `aliCreate`, `ZoneAdd`, and `CfgAdd` commands from a switch within the fabric for which the alias is being created. For example, issue commands from switch A for the top fabric, and from switch B for the bottom fabric.

---

6. The next alias is for controller A1_top. The command for this alias is:

   ```
   aliCreate "Controller A1_top", "0,4"
   ```

   This generates an alias named "Controller A1_top" with switch domain 0 and port number 4.

   Because E-Ports cannot be zoned, an alias is not needed for domain 0 port 1 in this example.

7. Save the configuration:

   ```
   cfgSave
   ```

Note: HP recommends that you use the `cfgShow` command after every `cfgSave` command to verify that the previous commands have been accepted.

---

8. The next alias to create is from switch B. Open a Telnet session to switch B.
9. Create the Host 1_B alias:

   ```
   aliCreate "Host 1_B", "0,2"
   ```

10. Create the controller A-1 bottom alias:

    ```
    aliCreate "Controller A1_bottom", "0,4"
    ```

11. Save the configuration:

    ```
    cfgSave
    ```

This completes alias naming for the Green Zones. The next section configures the Blue Zones.

Example: Zoning Blue Zone_Top and Blue Zone_Bottom

Zoning the Blue portion of this example is similar to the steps for the Green Zone, with a few name and number changes. See Table 20 for the sample Blue Zone_Top and Blue Zone_Bottom input form.

Table 20: Blue Zone_Top and Blue Zone_Bottom input form

Zoning Configuration Name=Top_Fabric

Zone Name=Blue Zone_Top **Switch Name=Switch Y** **Path=A**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	1	1	—	E-Port	Remote
	1	2	Host 2_Y	Host	Remote
	1	4	Controller Y1_top	Controller	Remote

Zoning Configuration Name=Bottom_Fabric

Zone Name=Blue Zone_Bottom **Switch Name=Switch Z** **Path=B**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	1	1	—	E-Port	Remote
	1	2	Host 2_Z	Host	Remote
	1	4	Controller Y1_bottom	Controller	Remote

As shown in Figure 33, the Host in the Blue Zone is named “Host 2."

1. Log the domain IDs of switches Y and Z. In this example, they are both Domain ID 1.

   Log this information in the Blue Zone_Top and Blue Zone_Bottom input form. On this input form, list the Blue Zone in two blocks, one for switch Y in Blue Zone_Top and one for switch Z in Blue Zone_Bottom. See Table 20 for entries.

2. Log the ports that connect to the hosts and E ports.

   Figure 33 shows that “Host 2” is the host name and that there are two connections from Host 2 to the switches. Host 2 path 2_Y is connected to port 2 of switch Y; Host 2 path 2_Z is connected to port 2 of switch Z. The E-Port is located in port 1 on both switches Y and Z.

3. List the controller connections for the top and bottom fabrics.

   Figure 33 shows that the controller pair is listed as Controller Y1_top (top controller, port 1), and Controller Y1_bottom (bottom controller, port 1). Switch Y port 4 connects to Controller Y1_top in the top fabric. Switch Z port 4 connects to Controller Y1_bottom in the bottom fabric.

4. Select the Telnet session from switch A.

5. Create the alias names in the zone.

   The naming convention in the example refers to Host 2_Y as the host name and path for the connection to port 2 of switch Y. The command for this alias is:

   ```
   aliCreate "Host 2_Y", "1,2"
   ```

   This generates an alias named “Host 2_Y,” with a switch domain of 1 and port number 2.

6. The next alias is for Controller Y1_top:

   ```
   aliCreate "Controller Y1_top", "1,4"
   ```

   This generates an alias named “Controller Y1_top,” with a switch domain of 1 and port number 4.

   Because E ports cannot be zoned, an alias is not needed for domain 1 port 1.

7. Save the configuration:

   ```
   cfgSave
   ```

8. The next alias to create is from switch Z. Open a Telnet session to switch B.

9. Create the Host 2_Z alias:

   ```
   aliCreate "Host 2_Z", "1,2"
   ```

10. Create the controller Y1_bottom alias:

    ```
    aliCreate "Controller Y1_bottom", "1,4"
    ```

11. Save the configuration:

    ```
    cfgSave
    ```

This completes the alias naming for the Blue Zones. The next section configures the Red Zones.

Example: Zoning Red Zone_Top and Red Zone_Bottom

Zoning the Red Zone portion of this example is similar to zoning the Blue and Green Zones, with a few exceptions. See Table 21 for the sample Red Zone_Top and Red Zone_Bottom input form.

Table 21: Red Zone_Top and Red Zone_Bottom input form

Zoning Configuration Name=Top_Fabric

Zone Name=Red Zone_Top **Switch Name=Switch A&Y** **Path=A&B**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	0	6	Controller A2_top	Controller	Local
	1	6	Controller Y2_top	Controller	Remote

Zoning Configuration Name=Bottom_Fabric

Zone Name=Red Zone_Bottom **Switch Name=Switch B&Z** **Path=A&B**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	0	6	Controller A2_bottom	Controller	Local
	1	6	Controller Y2_bottom	Controller	Remote

As shown in Figure 33, the Red Zone contains only switch ports and controller ports. It contains no hosts.

These are the DRM remote copy paths:

As shown earlier, switches A and B are Domain ID 0; switches Y and Z are Domain ID 1.

1. List switch domains A and Y in the Red Zone_Top input form. List switch Domains B and Z in the Red Zone_Bottom form.
2. List the controller connections.

   Figure 33 shows the controller pair listed as: Controller A2_top (top A controller, port 2) and Controller Y2_top (top Y controller, port 2).

   a. List these two connections in the Red Zone_Top input form.

   b. List Controller A2_bottom (meaning bottom A controller, port 2) and Controller Y2_bottom (meaning bottom Y controller, port 2) in the Red Zone_Bottom input form.

   Switch A, port 6 connects to Controller A2_top. Switch Y, port 6 connects to Controller Y2_top. Switch B, port 6 connects to Controller A2_bottom. Switch Z, port 6 connects to Controller Y2_bottom.
3. Select the Telnet session from switch A.
4. Create the alias names in the zone. For the connections from switches A and Y to the controllers A2_top and Y2_top, the commands are:

   ```
   aliCreate "Controller A2_top", "0,6"
   aliCreate "Controller Y2_top", "1,6"
   ```

   These commands create the alias “Controller A2_top” with Domain ID 0 and switch port 6; and the alias “Controller Y2_top” with Domain ID 1 and switch port 6.
5. Save the configuration:

   ```
   cfgSave
   ```
6. Select the Telnet session to switch B.
7. For the connections from switches B and Z to the controllers A2_bottom and Y2_bottom, enter the following commands:

   ```
   aliCreate "Controller A2_bottom", "0,6"
   aliCreate "Controller Y2_bottom", "1,6"
   ```

   These commands create the alias “Controller A2_bottom” with Domain ID 0 and switch port 6; and the alias “Controller Y2_bottom” with Domain ID 1 and switch port 6.
8. Save the configuration:

   ```
   cfgSave
   ```

Create the Zone Names

1. Select the Telnet session from switch A.
2. Create the Green Zone_Top name and add the zone members:

   ```
   zoneCreate "Green Zone_Top", "Host 1_A; Controller A1_top”
   ```

3. Create the Blue Zone_Top name and add the zone members:

   ```
   zoneCreate "Blue Zone_Top", "Host 2_Y; Controller Y1_top"
   ```

4. Create the Red Zone_Top name and add the zone members:

   ```
   zoneCreate "Red Zone_Top", "Controller A2_top; Controller Y2_top”
   ```

   These three steps create the zone names that are stored in flash memory in both switches A and Y. The next step is to repeat these commands for switches B and Z.

5. Save the configuration:

   ```
   cfgSave
   ```

6. Select the Telnet session from switch B.
7. Create the Green Zone_Bottom name and add the zone members:

   ```
   zoneCreate "Green Zone_Bottom", "Host 1_B; Controller A1_bottom"
   ```

8. Create the Blue Zone_Bottom name and add the zone members:

   ```
   zoneCreate "Blue Zone_Bottom", "Host 2_Z; Controller Y1_bottom"
   ```

9. Create the Red Zone_Bottom name and add the zone members:

   ```
   zoneCreate "Red Zone_Bottom", "Controller A2_bottom;
   Controller Y2_bottom"
   ```

   These three steps create the zone names that are stored in flash memory in both switches B and Z.

10. Save the configuration:

    ```
    cfgSave
    ```

Create the Configuration Name

1. Select the Telnet session from switch A.
2. Create the configuration using “Top_Fabric” as the example name and add all of the zone members. The command is:

   ```
   cfgCreate "Top_Fabric", "Green Zone_Top; Blue Zone_Top; Red Zone_Top"
   ```

   This creates a configuration file titled “Top_Fabric,” which contains Green Zone_Top, Blue Zone_Top, Red Zone_Top, and their alias members. These are stored in flash memory for switches A and Y.

3. Save the configuration:

   ```
   cfgSave
   ```

4. Enable the new zone configuration with the following command:

   ```
   cfgEnable "Top_Fabric"
   ```

   This now becomes the effective (in use) configuration for both switches A and Y.

5. To make this the active configuration after a restart or power-down, issue one final `cfgSave` command:

   ```
   cfgSave
   ```

This ensures the effective configuration of the switches after a restart or power-down.

6. Select the Telnet session from switch B.
7. Create the configuration using “Bottom_Fabric” as the filename and add all of the zone members. The command is:

   ```
   cfgCreate "Bottom_Fabric", "Green Zone_Bottom; Blue Zone_Bottom;
   Red Zone_Bottom"
   ```

   This creates a configuration file titled “Bottom_Fabric,” which contains Green Zone_Bottom, Blue Zone_Bottom, Red Zone_Bottom, and their alias members. these are stored in flash memory for switches B and Z.
8. Save the configuration:

   ```
   cfgSave
   ```
9. Enable the new zone configuration with the following command:

   ```
   cfgEnable "Bottom_Fabric"
   ```

   This now becomes the effective (in use) configuration for both switches B and Z.
10. To make this the active configuration after a restart or power-down, issue one final `cfgSave` command:

    ```
    cfgSave
    ```

    This ensures the effective configuration of the switches after a restart or power-down.

Zoning for a DRM homogeneous configuration is now complete.

DRM Heterogeneous Configuration

A DRM heterogeneous configuration consists of multiple operating systems sharing the same pair of storage arrays. A DRM heterogeneous configuration can be created from a DRM homogeneous configuration. This is done by adding zones that consist of new servers or clusters of a different operating system type from those in the original DRM homogeneous configuration. These new zones share the same storage arrays and isolate the additional operating system from the original operating system.

This section shows the steps to add zones from a DRM homogeneous configuration to create a DRM heterogeneous configuration. These same steps can be applied to an existing DRM heterogeneous configuration to add a new operating system.

If you are adding new zones to an existing DRM configuration, read from the beginning of this section, Zoning a DRM Configuration, page 185. This will help you understand the configuration examples and naming conventions. Figure 34 shows the additional four zones created. These zones are named, for this example, “Yellow Zone_Top” and “Yellow Zone_Bottom” (for the initiator site); “Brown Zone_Top” and “Brown Zone_Bottom” (for the target site). Use Figure 32 along with Figure 34 to picture the zoning scheme of a DRM heterogeneous configuration.

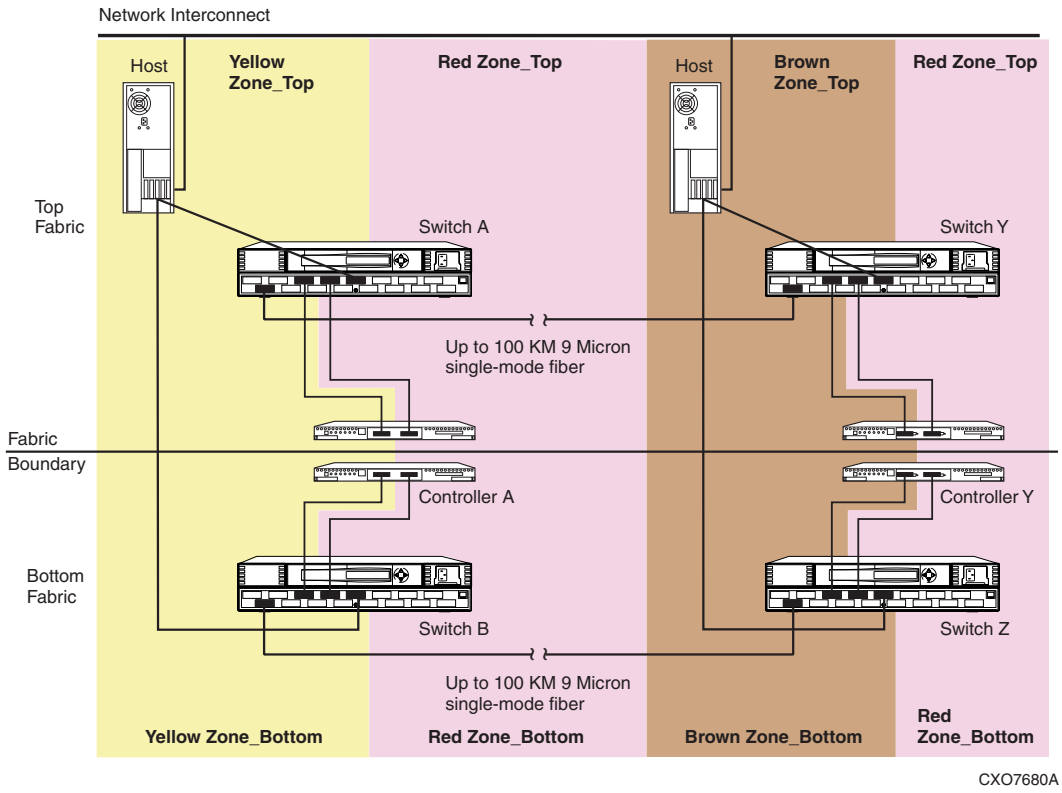


Figure 34: Zoning in a DRM heterogeneous environment

Use Table 18, the blank zoning input form template, to record and track the required device and command information. The form is designed to support two paths, two switches, and a maximum of 16 entries per switch. Copy and use a separate form to track information for each zone (such as Yellow Zone_Top, Brown Zone_Bottom, and so on). Organize alias name, function, and site data by either WWID number or Port ID number.

Figure 35 shows an example of the additional zones created for a DRM heterogeneous configuration.

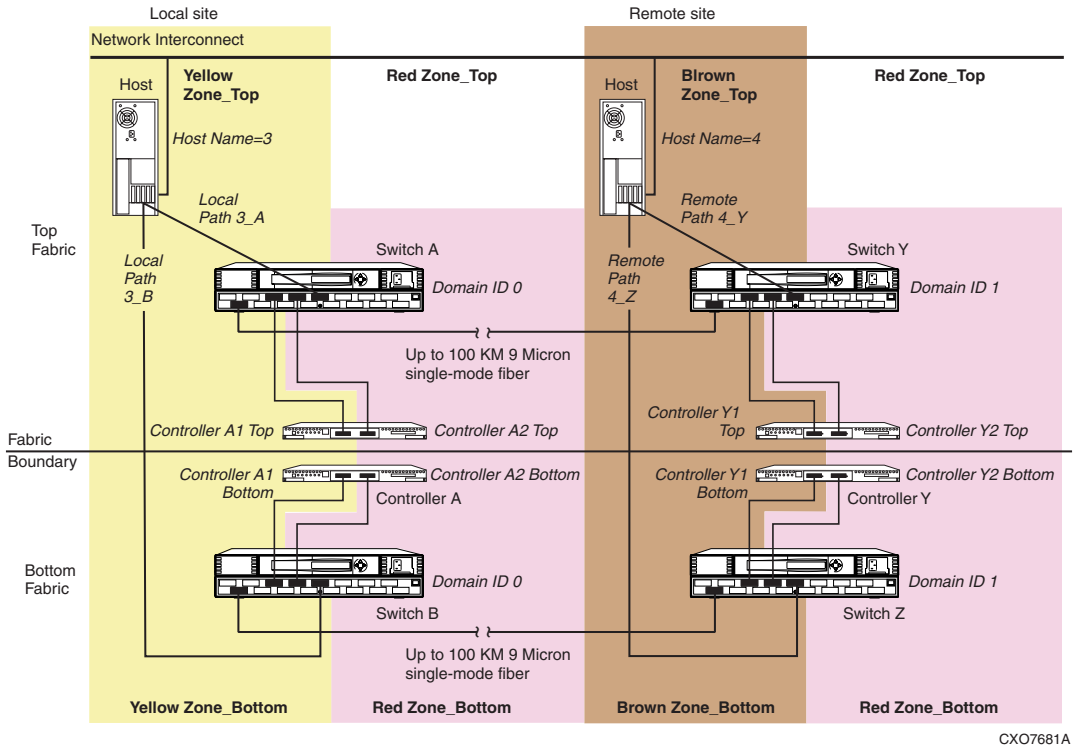


Figure 35: DRM example showing the new zones

The following sections contain the process that creates the zoning configuration illustrated in Figure 35. Because multiple configurations can be created and saved, the one currently in use is known as the *effective configuration*. The process to create and save an effective configuration (that ensures the switches are enabled after reboot or shutdown) includes the following:

1. Zoning the top fabric initiator site (designated “Yellow Zone_Top”)
2. Zoning the top fabric target site (designated “Brown Zone_Top”)
3. Zoning the two zones for the bottom fabric.

Two examples follow that illustrate these zoning concepts.

Example: Zoning Yellow Zone_Top and Yellow Zone_Bottom

Table 22, the Yellow Zone_Top and Yellow Zone_Bottom input form, is created from the blank template (Table 18) and is added to during this example.

Table 22: Yellow Zone_Top and Yellow Zone_Bottom input form

Zoning Configuration Name=Top_Fabric

Zone Name=Yellow Zone_Top **Switch Name=Switch A** **Path=A**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	0	1	—	E-Port	Local
	0	8	Host 3_A	Host	Local
	0	4	Controller A1_top	Controller	Local

Zoning Configuration Name=Bottom_Fabric

Zone Name=Yellow Zone_Bottom **Switch Name=Switch B** **Path=B**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	0	1	—	E-Port	Local
	0	8	Host 3_B	Host	Local
	0	4	Controller A1_bottom	Controller	Local

Table 22 shows zoning using the Domain ID number and Port number, rather than the WWID number. The WWID could also have been used. A general rule is that if you are changing connections within the DRM, use the WWID for zoning. If you are changing out hardware, use the Domain ID and Port number. The zoning procedure follows.

1. Identify and record the Domain ID of each switch. To get this information, use the `switchShow` command from each switch in a Telnet session or from the front console of each switch. The example in Figure 35 shows that switches A and B both have a Domain of 0.

   After recording this information on a blank template form, give it the zone name "Yellow Zone_Top." On the form, list the Yellow Zone in two blocks, one for switch A in Yellow Zone_Top and one for switch B in Yellow Zone_Bottom (see Table 22).

2. Record the ports that connect to the hosts and E ports.

   Figure 35 shows that "Host 3" is the host name and there are two connections from Host 3 to the switches. Host 3 path 3_A is connected to port 8 of switch A; Host 3 path 3_B is connected to port 8 of switch B. The E-Port is located in port 1 of both switches A and B.

3. List the controller connections for the top and bottom fabrics.

   In Figure 35, the controller pair is listed as Controller A1_top (top controller, port 1) and Controller A1_bottom (bottom controller, port 1). Switch A, port 4 connects to Controller A1_top in the top fabric. Switch B, port 4 connects to Controller A1_bottom in the bottom fabric.

4. Open a Telnet session to switch A.

5. Create the alias names in the zone. The naming convention in the example refers to Host 3_A as the host name and path used for the connection to port 8 of switch A. The command for this alias is:

   ```
   aliCreate "Host 3_A", "0,8"
   ```

   This command creates an alias named "Host 3_A" with switch domain 0 and port number 8.

Note: Be sure to issue all `aliCreate`, `ZoneAdd`, and `CfgAdd` commands from a switch within the fabric for which the alias is being created. For example, issue commands from switch A for the top fabric and from switch B for the bottom fabric.

The controller alias "Controller A1_Top" has already been created and does not need to be repeated. Because E ports cannot be zoned, an alias is not needed for domain 0, port 1 on switch A.

---

6. Save the configuration:

   ```
   cfgSave
   ```

Note: HP recommends that you issue a `cfgShow` command after every `cfgSave` and verify the previous commands.

---

7. The next alias to create is from switch B. Open a Telnet session to switch B.

8. Create the Host 3_B alias with the command:

   ```
   aliCreate "Host 3_B", "0,8"
   ```

Note: The controller alias "Controller A1_Bottom" has already been created and does not need to be repeated.

9. Save the configuration:

```
cfgSave
```

This completes alias naming for the Yellow Zones. The next section configures the Brown Zones.

Example: Zoning Brown Zone_Top and Brown Zone_Bottom

Zoning the Brown portion of this example is similar to zoning the Yellow portion, with a few name and number changes. Table 23 shows the sample Brown Zone_Top and Brown Zone_Bottom input form.

Figure 35 shows that the host in the Brown Zone is named "Host 4." The zoning procedure follows.

1. Record the domain IDs of switches Y and Z. In this example, they are both Domain ID 1.

   Record this information in the Brown Zone_Top and Brown Zone_Bottom input form. List the Brown Zone in two blocks, one for switch Y in Brown Zone_Top and one for switch Z in Brown Zone_Bottom. See Table 23 for entries.

2. Record the ports that connect to the hosts and E ports.

   Figure 35 shows that "Host 4" is the host name and that there are two connections from Host 4 to the switches. Host 4 path 4_Y is connected to port 8 of switch Y; Host 4 path 4_Z is connected to port 8 of switch Z. The E-Port is located in port 1 on both switches Y and Z.

3. List the controller connections for the top and bottom fabrics.

   Figure 35 shows that the controller pair is listed as Controller Y1_top (top controller, port 1) and Controller Y1_bottom (bottom controller, port 1). Switch Y port 4 connects to Controller Y1_top in the top fabric. Switch Z connects to Controller Y1_bottom in the bottom fabric.

4. Select the Telnet session from switch A.

5. Create the alias names in the zone.

   The naming convention in the example refers to "Host 4_Y" as the host name and path for the connections to port 8 of switch Y. The command to create this alias is:

```
aliCreate "Host 4_Y", "1,8"
```

   This command creates an alias named "Host 4_Y" with a switch domain of 1 and port number 8.

Note: The controller alias "Controller Y1_Top" has already been created and does not need to be repeated. Because E ports cannot be zoned, an alias is not needed for domain 1 port 1.

6. Save the configuration:

```
cfgSave
```

Table 23: Brown Zone_Top and Brown Zone_Bottom input form

Zoning Configuration Name=Top_Fabric

Zone Name=Brown Zone_Top **Switch Name=Switch Y** **Path=A**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	1	1	—	E-Port	Remote
	1	8	Host 4_Y	Host	Remote
	1	4	Controller Y1_top	Controller	Remote

Zoning Configuration Name=Bottom_Fabric

Zone Name=Brown Zone_Bottom **Switch Name=Switch Z** **Path=B**

WWID #	Domain ID #	Port #	Alias Name	Function	Site
	1	1	—	E-Port	Remote
	1	8	Host 4_Z	Host	Remote
	1	4	Controller Y1_bottom	Controller	Remote

7. The next alias to create is from switch Z. Open a Telnet session to switch B.
8. Create the Host 4_Z alias:

```
aliCreate "Host 4_Z", "1,8"
```

Note: The controller alias "Controller Y1_Bottom" has already been created and does not need to be repeated.

9. Save the configuration:

```
cfgSave
```

This completes alias naming for the Brown Zones.

Note: The Red Zones have already been created, so the port aliases for the Red Zone ports do not need to be repeated.

Create the Zone Names

1. Select the Telnet session from switch A.
2. Create the Yellow Zone_Top name and add the zone numbers:

```
zoneCreate "Yellow Zone_Top", Host 3_A; Controller A1-top"
```

3. Create the Brown Zone_Top name and add the zone numbers:

```
zoneCreate "Brown Zone_Top", "Host 4_Y; Controller Y1_top"
```

Note: Red Zone_Top has already been created and does not need to be repeated.

These two steps created the zone names that are stored in flash memory in both switches A and Y. The next step is to repeat these two commands for switches B and Z.

4. Save the configuration:

```
cfgSave
```

5. Select the Telnet session from Switch B.
6. Create the Yellow Zone_Bottom name and add the zone numbers:

```
zoneCreate "Yellow Zone_Bottom", "Host 3_B; Controller A1_Bottom
```

7. Create the Brown Zone_Bottom name and add the zone numbers:

```
zoneCreate "Brown Zone_Bottom", "Host 4_Z; Controller Y1_Bottom
```

Note: "Red Zone_Bottom" has already been created and does not need to be repeated.

These two steps created the zone names that are stored in flash memory in both switches B and Z.

8. Save the configuration:

```
cfgSave
```

Add the New Zones to the Configuration

1. Select the Telnet session from switch A.
2. Add the new top zones to the configuration Top_Fabric:

Note: Top_Fabric has already been created.

```
cfgAdd "Top_Fabric", "Yellow Zone_Top; Brown Zone_Top"
```

This adds Yellow Zone_Top and Brown Zone_Top to a configuration file titled "Top_Fabric," which already contains Green Zone_Top, Blue Zone_Top, Red Zone_Top, and their alias members. These are stored in flash memory for switches A and Y.

3. Save the configuration:

```
cfgSave
```

4. Enable the new zone configuration:

```
cfgEnable "Top_Fabric"
```

Note: This configuration now becomes the effective (in use) configuration for both switches A and Y.

5. To make this the active configuration after a restart or power-down, issue another `cfgSave` command:

```
cfgSave
```

This ensures the effective configuration of the switches after a restart or power-down.

6. Verify that the Top_Fabric configuration is correct:

```
cfgShow
```

The system produces a display of the Top_Fabric configuration similar to the following:

```
Defined configuration:
cfg: Top_Fabric
       Blue Zone_Top; Brown Zone_Top; Green Zone_Top;
       Red Zone_Top; Yellow Zone Top
zone: Blue Zone_Top
    . . . . . .                Host 2_Y; Controller Y1_top
zone: Brown Zone_Top
        Host 4_Y; Controller Y1_top
zone: Green Zone_Top
        Host 1_A; Controller A1_top
zone: Red Zone_Top
        Controller A2_top; Controller Y2_top
zone: Yellow Zone_Top
        Host 3_A; Controller A1_top
alias: Controller A1_top
        0,4
alias: Controller A2_top
        0,6
alias: Controller Y1_top
```

```
        1,4
alias: Controller Y2_top
        1,6
alias: Host 1_A
        0,2
alias: Host 2_Y
        1,2
alias: Host 3_A
        0,8
alias: Host 4_Y
        1,8
Effective configuration:
cfg:  Top_Fabric
zone: Blue Zone_Top
    . . . . . . . . . . . . . . . . . . . . . . . . . . . .        1,2
        1,4
zone: Brown Zone_Top
        1,8
        1,4
zone: Green Zone_Top
        0,2
        0,4
zone: Red Zone_Top
        0,6
        1,6
zone: Yellow Zone_Top
        0,8
        0,4
```

7. Select the Telnet session from switch B.
8. Add the new bottom zones to the configuration Bottom_Fabric:

Note: The Bottom_Fabric has already been created.

This adds Yellow Zone_Bottom and Brown Zone_Bottom to a configuration file titled "Bottom_Fabric," which already contains Green Zone_Bottom, Blue Zone_Bottom, Red Zone_Bottom, and their alias members. These are stored in flash memory for switches B and Z.

9. Save the configuration:

   ```
   cfgSave
   ```

10. Enable the new zone configuration:

    ```
    cfgEnable "Bottom_Fabric"
    ```

Note: This configuration now becomes the effective (in use) configuration for both switches B and Z.

11. To make this the active configuration after a restart or power-down, issue another `cfgSave` command:

    ```
    cfgSave
    ```

    This ensures the effective configuration of the switches after a restart or power-down.

12. Verify that the Bottom_Fabric configuration is correct:

    ```
    cfgShow
    ```

    The system produces a display of the Bottom_Fabric configuration similar to the following:

```
Defined configuration:
cfg: Bottom_Fabric
        Blue Zone_Bottom; Brown Zone_Bottom; Green Zone_Bottom
       Red Zone_Bottom; Yellow Zone_Bottom
zone: Blue Zone_Bottom
       Host 2_Z; Controller Y1_bottom
zone: Brown Zone_Bottom
       Host 4_Z; Controller Y1_bottom
zone: Green Zone_Bottom
       Host 1_B; Controller A1_bottom
zone: Red Zone_Bottom
       Controller A2_bottom; Controller Y2_bottom
zone: Yellow Zone_Bottom
       Host 3_B; Controller A1_bottom
alias: Controller A1_bottom
       0,4
alias: Controller A2_bottom
       0,6
alias: Controller Y1_bottom
       1,4
alias: Controller Y2_bottom
       1,6
alias: Host 1_B
       0,2
alias: Host 2_Z
       1,2
alias: Host 3_B
       0,8
alias: Host 4_Z
       1,8
```

```
Effective configuration:
cfg: Bottom_Fabric
zone: Blue Zone_Bottom
       1,2
       1,4
zone: Brown Zone_Bottom
       1,8
       1,4
zone: Green Zone_Bottom
       0,2
       0,4
zone: Red Zone_Bottom
       0,6
       1,6
zone: Yellow Zone_Bottom
       0,8
       0,4
```

Zoning for a DRM heterogeneous configuration is now complete. If you want to add additional zones, repeat the steps starting at the section titled "DRM Heterogeneous Configuration."

Zoning to Allow Host Access Between Sites

The previous examples in this chapter are zoned so that the hosts at one site do not have access to controllers at the other site. The following example shows how to enable access of Host 1 in the Green Zone by Controller Y and Host 2 in the Blue Zone by Controller A.

1. Open a Telnet session to switch A.
2. Add a new zone member of Controller Y's top port 1 to the Green Zone Top:

   ```
   zoneAdd "Green Zone_Top","Controller Y1_top
   ```
3. Add a new zone member of Controller A's top port 1 to the Blue Zone Top:

   ```
   zoneAdd "Blue Zone_Top","Controller A1_top
   ```
4. Enable the new zone configurations:

   ```
   cfgEnable "Top_Fabric"
   ```
5. Save the configuration:

   ```
   cfgSave
   ```
6. Open a Telnet session to switch B.
7. Add a new zone member of Controller Y's bottom port 1 to the Green Zone Bottom:

   ```
   zoneAdd "Green Zone_Bottom","Controller Y1_bottom"
   ```
8. Add a new zone member of Controller A's bottom port 1 to the Blue Zone Bottom:

   ```
   zoneAdd "Blue Zone_Bottom","Controller A1_bottom"
   ```
9. Enable the new zone configurations:

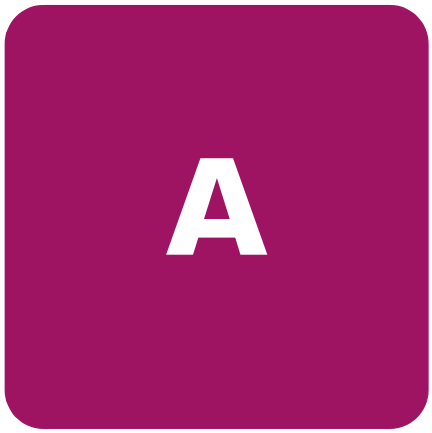
   ```
   cfgEnable "Bottom_Fabric"
   ```

10. Save the configuration:

```
cfgSave
```

Controller members from one site have now been added to the host zones at the other site. Repeat the procedure if other zones at one site need access to controllers at the other site.

Status Comparison



This appendix describes the procedure for comparing the status of:

- Controllers
- Association sets
- Remote copy sets
- Units
- Connections

Performing a status comparison consists of the following procedures:

- Target Site Terminal Emulator Session
- Issuing `SHOW` Commands

Target Site Terminal Emulator Session

1. Using a serial cable, connect the COM port of a laptop computer or another computer to the corresponding serial port on the HSG80 controllers.
2. Start a terminal emulator session that is capable of capturing text to a file (which is later saved as step 6 of the SHOW Commands procedure). Use the following settings: 9600 baud, 8 bits, no parity, 1 stop bit, XON/XOFF.

Issuing SHOW Commands

1. To see the full information on this controller, issue the CLI command:

   ```
   SHOW THIS_CONTROLLER FULL
   ```

   You should see a display similar to that shown in Example Display 1.
2. To see the information for all association sets known to the controller pair, issue the CLI command:

   ```
   SHOW ASSOCIATIONS FULL
   ```

   You should see a display similar to that in Example Display 2 for each association set.
3. To see information for all remote copy sets known to the controller pair, issue the CLI command:

   ```
   SHOW REMOTE_COPY FULL
   ```

   You should see a display similar to that in Example Display 3 for each remote copy set.
4. To see information for all units configured to the controller, issue the CLI command:

   ```
   SHOW UNITS FULL
   ```

   You should see a display similar to that in Example Display 4 for each unit.
5. To see the connection name, operating system, controller, controller port, adapter ID address, online or offline status, and unit offset, issue the CLI command:

   ```
   SHOW CONNECTIONS
   ```

   You should see a display similar to that in Example Display 5 for each connection.
6. Print and save two copies of the file started during the terminal emulator session procedure (step 2). Save one copy at each site. This file contains the text captured in steps 1-5 of the SHOW commands.

Example Display 1 corresponds to step 1 of the “Issuing SHOW Commands” section:

Example Display 1

```
Controller:
        HSG80 ZG91412410 Software V85P, Hardware  E05
        NODE_ID          = nnnnnnnnnnn
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
        Configured for MULTIBUS_FAILOVER with ZG91416136
            In dual-redundant configuration
        Device Port SCSI address 6
        Time: NOT SET
        Command Console LUN is lun 0 (NOIDENTIFIER)
```

```
Host PORT_1:
        Reported PORT_ID = 5000-1FE1-0001-3AE1
        PORT_1_TOPOLOGY  = FABRIC (fabric up)
        Address          = 220113
Host PORT_2:
        Reported PORT_ID = 5000-1FE1-0001-3AE2
        PORT_2_TOPOLOGY  = FABRIC (fabric up)
        Address          = 220313
        REMOTE_COPY = BuildingB
Cache:
        256 megabyte write cache, version 0012
        Cache is GOOD
        No unflushed data in cache
        CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
Mirrored Cache:
        256 megabyte write cache, version 0012
        Cache is GOOD
        No unflushed data in cache
Battery:
        NOUPS
        FULLY CHARGED
        Expires:
Extended information:
        Terminal speed 9600 baud, eight bit, no parity, 1 stop bit
       Operation control: 00000000  Security state code: 75184
      Configuration backup disabled
```

Example Display 2 corresponds to step 2 of the “Issuing SHOW Commands” section:

Example Display 2

```
Name          Association                    Uses             Used by
-------------------------------------------------------------------------
AS1           association                    RC1
                                             RC2
                                             RC3
        Switches:
          NOFAIL_ALL
          NOORDER_ALL
          NOLOG_UNIT
```

Example Display 3 corresponds to step 3 of the “Issuing SHOW Commands” section:

Example Display 3

```
Name                                          Uses             Used by
------------------------------------------------------------------------
RC1           remote copy             D1             AS1
        Reported LUN ID: nnnnnnnnnnnnnnn
        Switches:
          OPERATION_MODE  = SYNCHRONOUS
          ERROR_MODE      = NORMAL
          FAILOVER_MODE   = MANUAL
          OUTSTANDING_IOS = 60
                               .
                               .
                               .
```

Example Display 4 corresponds to step 4 of the “Issuing SHOW Commands” section:

Example Display 4

```
D2                                          DISK10100      BuildingB\RC2
        LUN ID: nnnnnnnnnnnnnnnnnnnnn
        NOIDENTIFIER
        Switches:
          RUN                    NOWRITE_PROTECT        READ_CACHE
          READAHEAD_CACHE        WRITEBACK_CACHE
          MAXIMUM_CACHED_TRANSFER_SIZE = 1
        Access:
    BuildngAA, BuildngAB, BuildngAC, BuildngAD, HostCon_1, HostCon_2
        State:
          ONLINE to this controller
          Not reserved
          PREFERRED_PATH = OTHER_CONTROLLER
          Target NORMAL
        Size:             17769177 blocks

    Geometry (C/H/S): ( 5258 / 20 / 169 )
```

Example Display 5 corresponds to step 5 of the “Issuing SHOW Commands” section:

Example Display 5

```
Connection                                              Unit
Name Operating system Controller  Port    Address    Status
Offset !NEWCON28 WINNT        THIS       1      634000    OL this       0
           HOST_ID=1000-0000-C921-4B5B ADAPTER_ID=1000-0000-C921-4B5B.
```

Replicating Storage Units

B

This chapter describes Data Replication Manager (DRM) concepts and procedures for making point-in-time copies of a storage unit.

The topics discussed in this chapter are:

- Cloning Data for Backup, page 217
- Snapshot, page 219

Cloning and *snapshot* are methods of making a point-in-time copy of a storage unit. Table 24 provides an overview comparison of the two methods.

Table 24: Cloning and Snapshot Comparison

Cloning	Snapshot
Can be performed at initiator site or target site.	Can be performed at target site only.
A physical copy that resides on disk. Can be a source for another clone. Source and cloned units.	A virtual copy that resides on disk and in cache. May not be snapped or cloned. Requires 512 MB cache for both controllers.
Read/write capability	Read/write capability
Data captured in hours (for moderate I/O loads, possibly at a rate of 60 GB/hour).	Data captured in seconds.
Can make four at a time per 6-member mirrorset. Limited by number of drives and number of mirrorsets allowed at any one time.	Four snapshot units allowed per storage array. One per source unit at any one time.
The source unit must have write-back cache disabled.	The source unit must have the following characteristics: Less than 512 GB Write-back cache enabled Nontransportable Requires ACS Version 8.7S or 8.7P

Table 24: Cloning and Snapshot Comparison (Continued)

Cloning	Snapshot
Can clone an unpartitioned single-disk unit, stripeset, or mirrorset.	The snapshot unit must have the following characteristics: Write-back cache enabled Capacity equal to or greater than the source unit Made of any storage container except write history log containers
Source unit and clone both reside on and fail over on the same controller.	Source unit and snapshot unit both reside on and fail over on the same controller.
Operates in both multibus and controller failover modes.	Operates in both multibus and controller failover modes.

Cloning Data for Backup

Use the *CLONE* utility to duplicate data on any unpartitioned single-disk unit, stripeset, mirrorset, or striped mirrorset in preparation for backup. When the cloning operation is done, you can back up the clones rather than the storageset or the single-disk unit, which can continue to service its I/O load. When you are cloning a mirrorset, *CLONE* does not need to create a temporary mirrorset. Instead, it adds a temporary member to the mirrorset and copies the data to this new member.

The *CLONE* utility creates a temporary, two-member mirrorset for each member in a single-disk unit or stripeset. Each temporary mirrorset contains one disk drive from the unit you are cloning, and one disk drive to which *CLONE* copies the data. During the copy operation, the unit remains online and active, so the clones contain the most up to date data.

After the *CLONE* utility copies the data from the members to the clones, it restores the unit to its original configuration and creates a clone unit you can back up. The *CLONE* utility uses the steps shown in Figure 36 to duplicate each member of a unit.

Use the following steps to clone a single-disk unit, stripeset, or mirrorset:

1. Establish a connection to the controller that accesses the unit you want to clone.
2. Start *CLONE* using the command:

   ```
   RUN CLONE
   ```

3. When prompted, enter the unit number of the unit you want to clone.
4. When prompted, enter a unit number for the clone unit that *CLONE* will create.
5. When prompted, indicate how you would like the clone unit to be brought online: either automatically or only after your approval.
6. When prompted, enter the disk drives you want to use for the clone units.
7. Back up the clone unit.

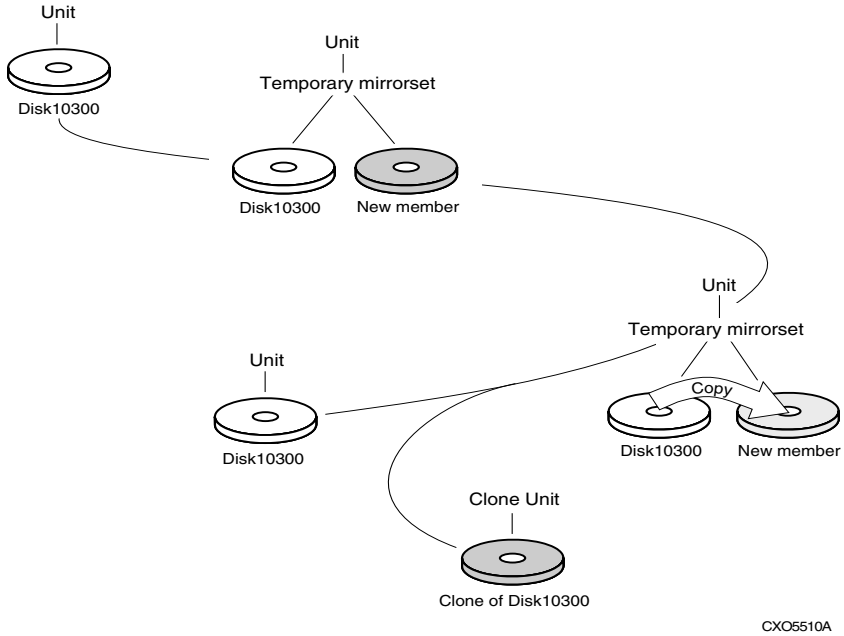


Figure 36: Steps the *CLONE* utility follows for duplicating unit members

Example: This example shows the commands you would use to clone storage unit D98. The *CLONE* utility terminates after it creates storage unit D99, a clone or copy of D98. Bold type indicates user entry.

```
RUN CLONE
CLONE LOCAL PROGRAM INVOKED
UNITS AVAILABLE FOR CLONING: 98
ENTER UNIT TO CLONE ? 98
CLONE WILL CREATE A NEW UNIT WHICH IS A COPY OF UNIT 98.
ENTER THE UNIT NUMBER WHICH YOU WANT ASSIGNED TO THE NEW UNIT ? 99
THE NEW UNIT MAY BE ADDED USING ONE OF THE FOLLOWING METHODS:
   1. CLONE WILL PAUSE AFTER ALL MEMBERS HAVE BEEN COPIED. THE USER MUST THEN
 PRESS RETURN TO CAUSE THE NEW UNIT TO BE ADDED.
   2. AFTER ALL MEMBERS HAVE BEEN COPIED, THE UNIT WILL BE ADDED AUTOMATICALLY.
    UNDER WHICH ABOVE METHOD SHOULD THE NEW UNIT BE ADDED[ ]? 1
    DEVICES AVAILABLE FOR CLONE TARGETS:
    DISK20200 (SIZE=832317)
    DISK20300 (SIZE=832317)
    DISK30100 (SIZE=832317)
    USE AVAILABLE DEVICE DISK20200(SIZE=832317) FOR MEMBER
DISK10300(SIZE=832317) (Y,N) [Y] ? Y
    MIRROR DISK10300 C_MA
    SET C_MA NOPOLICY
    SET C_MA MEMBERS=2
    SET C_MA REPLACE=DISK20200
    DEVICES AVAILABLE FOR CLONE TARGETS:
    DISK20300 (SIZE=832317)
    DISK30100 (SIZE=832317)
USE AVAILABLE DEVICE DISK10400(SIZE=832317) FOR MEMBER DISK(SIZE=832317)
    (Y,N) [Y] ?  Y
    MIRROR DISK10000 C_MB
    SET C_MB NOPOLICY
    SET C_MB MEMBERS=2
    SET C_MB REPLACE=DISK10400
    COPY IN PROGRESS FOR EACH NEW MEMBER. PLEASE BE PATIENT...
    .
    .
    COPY FROM DISK10300 TO DISK20200 IS 100% COMPLETE
    COPY FROM DISK10000 TO DISK10400 IS 100% COMPLETE

    PRESS RETURN WHEN YOU WANT THE NEW UNIT TO BE CREATED
    REDUCE  DISK20200 DISK10400
    UNMIRROR DISK10300
    UNMIRROR DISK10000
    ADD MIRRORSET C_MA       DISK20200
    ADD MIRRORSET C_MB       DISK10400
    ADD STRIPESET C_ST1  C_MA C_MB
    INIT C_ST1     NODESTROY
```

```
ADD UNIT D99 C_ST1
D99 HAS BEEN CREATED. IT IS A CLONE OF D98.
CLONE - NORMAL TERMINATION
```

Snapshot

With snapshot, the contents of a source unit are frozen in time and presented to the host as a second unit, the *snapshot*. The snapshot unit (Figure 37) preserves the original data (from the time of the snapshot) while allowing writes to the source unit to continue. A temporary volume (the snapshot unit) is created and used to store the original data that has been overwritten on the source unit since the time of the snapshot.

Using a cache bitmap, reads are directed to the source unit or the snapshot unit.

If no data has been written to the source unit since the time of the snapshot, data is then read from the source unit.

If data has been written to the source unit, then data is read from the snapshot unit.

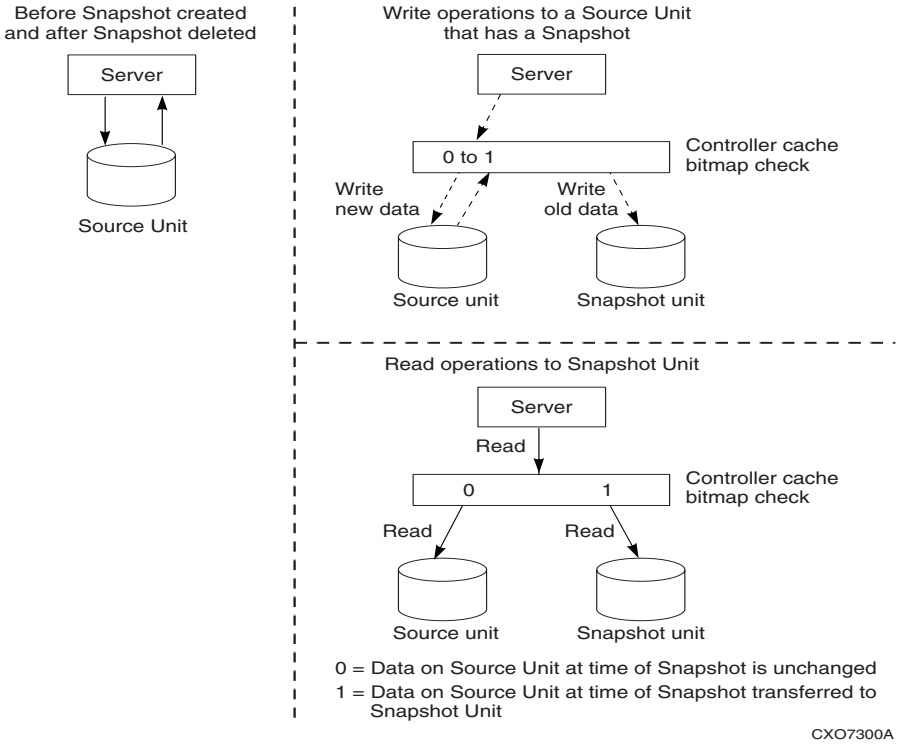


Figure 37: Snapshot unit

Snapshot Command

Note: This command is operational only in controller software versions 8.7S and 8.7P and is operational only if both controllers have 512 MB of mirrored cache.

This command creates and names a snapshot unit. A snapshot unit is one that reflects the contents of another unit at a specific time (the instant the ADD SNAPSHOT_UNITS command is entered). The snapshot unit can then be presented to the host. The snapshot unit remains until it is deleted (DELETE command).

Syntax

```
ADD SNAPSHOT_UNITS snapshot-unit storageset source-unit
```

Parameters

The following parameters are required for the ADD SNAPSHOT_UNITS command:

- Snapshot unit
- Storageset
- Source unit

When the ADD SNAPSHOT_UNITS command is entered, *storageset* becomes *snapshot-unit* and archives the current contents of *source-unit* at that instant.

These parameters are described in the paragraphs that follow.

snapshot-unit

The unit number assigned to the snapshot unit. The unit number must start with a letter (A through Z) and may consist of a maximum of nine characters, including letters A through Z, numerals 0 through 9, periods (.), dashes (-), and underscores (_).

Note: If you use scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention—use underscores instead. Dashes are not allowed by the Perl scripting language.

The snapshot unit is created with all host access disabled by default. Issue a SET command to set up host access.

The snapshot unit is created on the same controller as the source unit and must remain there.

storageset

Identifies the storageset that becomes the snapshot unit. The storageset must:

- Have a capacity equal to or greater than the source unit
- Be initialized
- Not be a partition or a concatset

Source unit

The unit whose contents is frozen in time and preserved on the snapshot unit. The source unit must:

- Be less than 512 GB
- Have write-back cache enabled
- Be nontransportable

Switches

There are no switches associated with this command.

Example

To create unit D4 (snapshot unit), which consists of storageset RAID2, and which becomes a point-in-time snapshot of unit D1 (source unit), enter:

```
ADD SNAPSHOT_UNITS D4 raid2 D1
```

Upgrading to ACS Version 8.7P Software

C

Array Controller Software (ACS) Version 8.7P implements the Data Replication Manager (DRM) feature, which can be upgraded using either a rolling or a shutdown upgrade method. These upgrade methods apply only to dual-redundant controller configurations.

Note: The rolling upgrade procedure is not currently supported for Microsoft Windows NT, Microsoft Windows 2000, and IBM AIX platforms. The shutdown upgrade procedure must be used for these platforms.

The rolling upgrade procedure is also not supported for an upgrade from Version 8.5P to Version 8.7P or for Version 8.6F, 8.6G, 8.6L, or 8.6S upgrade to Version 8.7P. Use the Shutdown Upgrade Procedure on page 231 instead.

The topics discussed in this chapter are:

- Rolling Upgrade Procedure for Version 8.6-xP to 8.7P, page 224
  - Initiator Site Upgrade Procedure, page 224
  - Target Site Upgrade Procedure, page 228
  - Completion of the Initiator Site Upgrade Procedure, page 231
- Shutdown Upgrade Procedure for 8.7P, page 231
  - Initiator Site Shutdown Upgrade Procedure, page 231
  - Target Site Shutdown Upgrade Procedure, page 234
  - Completion of Initiator Site Shutdown Upgrade Procedure, page 236

Rolling Upgrade Procedure for Version 8.6-xP to 8.7P

The ACS Version 8.7P rolling upgrade procedure from ACS Version 8.6-xP allows the disk to be accessible during the upgrade process with minimal disruption. Specific controllers are referred to as Controller A or Controller B during the procedure. For clarity, the CLI prompts illustrated in the procedure use *HSGA*> and *HSGB*> to indicate the controller used.

Note: The steps in this procedure *must* be followed exactly for the upgrade procedure to work properly. This procedure takes 10 to 20 minutes per site, depending on the complexity of the configuration. The units involved are briefly unavailable twice during the procedures for 10 to 20 seconds in step 11 and step 13.

In the procedures that follow, initiator site procedure steps are marked with an initiator symbol, ▻. Target site procedures are marked with a target symbol, ⊙.

The rolling upgrade procedure upgrades the initiator site controllers to a specific point and then fully upgrades the target site controllers before finalizing the upgrade for the initiator site controllers.

Initiator Site Upgrade Procedure

Begin the rolling upgrade by executing the following procedure on the initiator site controllers.

▻ 1. Connect a PC or terminal to the maintenance port of Controller A at the initiator site. If you cannot find the ACS Version 8.6 configuration, perform the process in Appendix A now.

▻ 2. Delete any snapshot units by performing the following steps:

   a. Identify all snapshot units:

      ```
      HSGA> SHOW UNITS FULL
      ```

   b. Record the configuration for each snapshot unit for later restoration.

   c. Delete all snapshot units individually with the following command:

      ```
      HSGA> DELETE snapshot-unit-name
      ```

▻ 3. Verify that all snapshot units are deleted:

   ```
   HSGA> SHOW UNITS FULL
   ```

Note: If any snapshot unit remains, repeat step 2.

---

4. Identify and record the current CACHE_FLUSH_TIMER value:

   ```
   HSGA> SHOW THIS_CONTROLLER
   ```

   The following text is only a portion of the resulting display:

   ```
   Cache:
           256 megabyte write cache, version 0022
           Cache is GOOD
           No unflushed data in cache
           CACHE_FLUSH_TIMER=DEFAULT (10 seconds)
   ```

Note: The CACHE_FLUSH_TIMER value is displayed in the caching parameters section. This parameter is modified during the procedure and must be restored later.

5. For each unit, identify and record the unit WRITEBACK_CACHE characteristics by issuing the following command:

   ```
   HSGA> SHOW UNITS FULL
   ```

Note: The unit WRITEBACK_CACHE characteristics are modified during the upgrade procedure and must be restored later.

6. Set the CACHE_FLUSH_TIMER to 1 second to minimize the flush time:

   ```
   HSGA> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=1
   HSGA> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=1
   ```

7. Disable writeback caching on all units (to help minimize failover time) by issuing the following command as required for each unit:

   ```
   HSGA> SET unit-name NOWRITEBACK_CACHE
   ```

8. Determine whether all data has been flushed from the cache module:

   ```
   HSGA> SHOW THIS_CONTROLLER
   ```

   The following text is only a portion of the resulting display:

   ```
   Cache:
           256 megabyte write cache, version 0022
           Cache is GOOD
           No unflushed data in cache
           CACHE_FLUSH_TIMER=1 SECOND
   ```

Note: Repeat this step on both controllers (THIS_CONTROLLER and OTHER_CONTROLLER) until no unflushed data remains in either cache module memory.

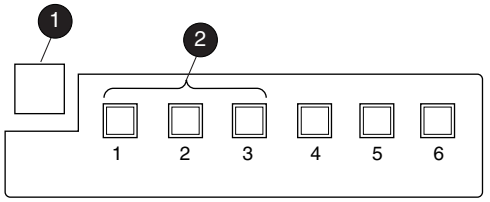
If unwritten data is present after 15 minutes, verify that WRITEBACK_CACHE is disabled on all units by issuing the `SHOW UNITS FULL` command. For any units with WRITEBACK_CACHE enabled, return to step 7 and proceed.

9. Shut down Controller B:

```
HSGA> SHUTDOWN OTHER_CONTROLLER
```

Note: Disregard any messages about misconfigured controllers or failover status.

After Controller B shuts down, the **Reset** button and the first three LEDs turn on (see Figure 38). Proceed only after the **Reset** button stops flashing and remains on.



❶ **Reset** button
❷ First three LEDs

CXO6991A

Figure 38: Controller reset button and first three LEDs

10. Verify that all units failed over to Controller A:

```
HSGA> SHOW UNITS FULL
```

The following text is only a portion of the resulting display:

```
State:
        ONLINE to this controller
        Not reserved
```

11. Upgrade the software on Controller B by performing the following steps:

Note: After this step has been performed, the previous ACS version cannot be restored to this subsystem without performing the downgrade process, which should be performed only by HP authorized service personnel.

a. Remove the program card ESD cover from Controller B.
b. While pressing and holding the controller **Reset** button, eject the old program card.
c. After ejecting the program card, release the **Reset** button.
d. While pressing and holding the controller **Reset** button, insert the new program card.
e. After the card is fully inserted, release the button. Controller B restarts.

Note: A controller restart can take as long as 60 seconds and is indicated by the temporary cycling of the port LEDs and a flashing **Reset** button. Disregard messages about misconfigured controllers or failover status. When controller B has restarted, it automatically shuts down Controller A.

f. Install the program card ESD cover on Controller B.

12. Verify that Controller B completed initialization:
    a. Connect the PC or terminal to the maintenance port of Controller B.
    b. Make sure that the CLI prompt for Controller B appears.

Note: Wait for the CLI prompt before proceeding.

    c. Verify that Controller A is shut down: the **Reset** button and the first three LEDs turn on (see Figure 38 on page 226). Proceed only after the **Reset** button stops flashing and remains on.

13. Upgrade the software on Controller A by performing the following steps:
    a. Remove the program card ESD cover from Controller A.
    b. While pressing and holding the controller **Reset** button, eject the old program card.
    c. After ejecting the program card, release the **Reset** button.
    d. While pressing and holding the controller **Reset** button, insert the new program card.
    e. After the card is fully inserted, release the button. Controller A restarts.

Note: A controller restart can take as long as 60 seconds and is indicated by the temporary cycling of the port LEDs and a flashing **Reset** button. Disregard messages about misconfigured controllers or failover status.

    f. Install the program card ESD cover on Controller A.

Caution: Stop upgrading the initiator site controllers at this point and proceed to upgrade the target site controllers. Failure to upgrade the target site controllers at this point could cause the initiator and target site controllers to crash and prevent the host from accessing data storage in these subsystems.

The initiator site upgrade procedure continues on page 231 after the target site upgrade procedure.

Continue the rolling upgrade by executing the following procedure on the target site controllers.

Target Site Upgrade Procedure

Note: During the target site upgrade, one of the initiator site controllers could restart with an instance code of 0xE096980. This potential restart is expected; disregard the associated instance code.

1. Connect a PC or terminal to the maintenance port of Controller A at the target site.
2. Delete any snapshot units by performing the following steps:
   a. Identify all snapshot units:

      ```
      HSGA> SHOW UNITS FULL
      ```

   b. Record the configuration for each snapshot unit for restoration in step 16.
   c. Delete all snapshot units individually with the following command:

      ```
      HSGA> DELETE snapshot-unit-name
      ```

3. Verify that all snapshot units are deleted:

   ```
   HSGA> SHOW UNITS FULL
   ```

Note: If any snapshot unit remains, repeat step 2.

4. Identify and record the current CACHE_FLUSH_TIMER value:

   ```
   HSGA> SHOW THIS_CONTROLLER
   ```

   The following text is only a portion of the resulting display:

   ```
   Cache:
           256 megabyte write cache, version 0022
           Cache is GOOD
           No unflushed data in cache
           CACHE_FLUSH_TIMER=DEFAULT (10 seconds)
   ```

Note: The CACHE_FLUSH_TIMER value is displayed in the caching parameters section. This parameter is modified during the procedure and must be restored in step 14.

5. For each unit, identify and record the unit WRITEBACK_CACHE characteristics:

   ```
   HSGA> SHOW UNITS FULL
   ```

Note: The unit WRITEBACE_CACHE characteristics are modified during the upgrade procedure and must be restored in step 15.

6. Set the CACHE_FLUSH_TIMER to 1 second with the following commands:

```
HSGA> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=1
HSGA> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=1
```

7. Disable writeback caching on all units to help minimize failover time. Issue the following command as required for each unit:

```
HSGA> SET unit-name NOWRITEBACK_CACHE
```

8. Determine whether all data has been flushed from the cache module:

```
HSGA> SHOW THIS_CONTROLLER
```

The following text is only a portion of the resulting display:

```
Cache:
        256 megabyte write cache, version 0022
        Cache is GOOD
        No unflushed data in cache
        CACHE_FLUSH_TIMER=1 SECOND
```

Note: Repeat this step on both controllers (THIS_CONTROLLER and OTHER_CONTROLLER) until no unflushed data remains in either cache module memory.

If unwritten data is present after 15 minutes, verify that WRITEBACK_CACHE was disabled on all units by issuing the `SHOW UNITS FULL` command. For any units with WRITEBACK_CACHE enabled, return to step 7 and proceed from there.

---

9. Shut down Controller B:

```
HSGA> SHUTDOWN OTHER_CONTROLLER
```

Note: Disregard any messages about misconfigured controllers or failover status.

After Controller B shuts down, the **Reset** button and the first three LEDs turn on (see Figure 38 on page 226). Proceed only after the **Reset** button stops flashing and remains on.

---

10. Verify that all units failed over to Controller A by issuing the following command to show the status of each unit:

```
HSGA> SHOW UNITS FULL
```

The following text is only a portion of the resulting display:

```
State:
        ONLINE to this controller
        Not reserved
```

11. Upgrade the software on Controller B by performing the following steps.

Note: After this step has been performed, the previous ACS version cannot be restored to this subsystem without performing the downgrade process, which should be performed only by HP authorized service personnel.

a. Remove the program card ESD cover from Controller B.
b. While pressing and holding the controller **Reset** button, eject the old program card.
c. After ejecting the program card, release the **Reset** button.
d. While pressing and holding the controller **Reset** button, insert the new program card.
e. After the card is fully inserted, release the button. Controller B restarts.

Note: A controller restart can take as long as 60 seconds and is indicated by the temporary cycling of the port LEDs and a flashing **Reset** button. Disregard messages about misconfigured controllers or failover status. When controller B has restarted, it automatically shuts down Controller A.

f. Install the program card ESD cover on Controller B.

12. After Controller B restarts, verify that Controller B completed initialization:
    a. Connect the PC or terminal to the maintenance port of Controller B.
    b. Make sure that the CLI prompt for Controller B appears.

Note: Wait for the CLI prompt before proceeding.

c. Verify that controller A is shut down; the **Reset** button and the first three LEDs turn on (see Figure 38 on page 226). Proceed only after the **Reset** button stops flashing and remains on.

13. Upgrade the software on controller A by performing the following steps:
    a. Remove the program card ESD cover from Controller A.
    b. While pressing and holding the controller **Reset** button, eject the old program card.
    c. After ejecting the program card, release the **Reset** button.
    d. While pressing and holding the controller **Reset** button, insert the new program card.
    e. After the card is fully inserted, release the button. Controller A restarts.

Note: A controller restart can take as long as 60 seconds and is indicated by the temporary cycling of the port LEDs and a flashing **Reset** button. Disregard messages about misconfigured controllers or failover status.

f. Install the program card ESD cover on Controller A.

14. After Controller A restarts, restore the CACHE_FLUSH_TIMER to the value recorded in step 4 using the following commands:

```
HSGA> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=n
HSGA> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=n
```

15. For each unit, restore the WRITEBACK_CACHE settings as recorded in step 5:

```
HSGA> SET unit-name WRITEBACK_CACHE
```

16. Restore all snapshot units removed in step 2.

17. Disconnect the PC or terminal from the maintenance port of Controller A.

Completion of the Initiator Site Upgrade Procedure

1. After Controller A restarts, restore the CACHE_FLUSH_TIMER to the value recorded in step 4 on page 225:

```
HSGA> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=n
HSGA> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=n
```

2. For each unit, restore the writeback_cache settings as recorded in step 5 on page 225:

```
HSGA> SET unit-name WRITEBACK_CACHE
```

3. Restore all snapshot units removed in step 2 on page 224.

4. Disconnect the PC or terminal from the maintenance port of Controller A.

This completes the rolling upgrade to ACS Version 8.7P software.

Shutdown Upgrade Procedure for 8.7P

Specific controllers are referred to as Controller A or Controller B in this procedure. For clarity, the CLI prompts illustrated in this procedure use *HSGA*> and *HSGB*> to indicate which controller (A or B) is used.

Note: The steps in this procedure *must* be followed exactly for the upgrade procedure to work properly. This procedure takes 5 to 10 minutes per site. The units involved are unavailable during the upgrade procedure.

Use this procedure when upgrading from ACS Version 8.5. It must also be used for upgrading from Version 8.6F, 8.6G, 8.6L, or 8.6S to allow for rewiring of the fabrics into a DRM-supported configuration.

Initiator Site Shutdown Upgrade Procedure

Begin the shutdown upgrade using the following procedure on the initiator site controllers:

1. From a host console, stop all host activity to the controllers and dismount the logical units in the subsystem.

2. Connect a PC or terminal to the maintenance port of Controller A at the initiator site.

3. Delete any snapshot units by performing the following steps:

   a. Identify all snapshot units:

```
HSGA> SHOW UNITS FULL
```

b. Record the configuration for each snapshot unit for later restoration.

c. Delete all snapshot units individually with the following command:

```
HSGA> DELETE snapshot-unit-name
```

4. Verify that all snapshot units are deleted:

```
HSGA> SHOW UNITS FULL
```

Note: If any snapshot unit exists, repeat step 3.

5. Identify and record the current CACHE_FLUSH_TIMER value:

```
HSGA> SHOW THIS_CONTROLLER
```

The following text is only a portion of the resulting display:

```
Cache:
        256 megabyte write cache, version 0022
        Cache is GOOD
        No unflushed data in cache
        CACHE_FLUSH_TIMER=DEFAULT (10 seconds)
```

Note: The CACHE_FLUSH_TIMER value appears in the caching parameters section. This parameter is modified during the procedure and must be restored later.

6. Set the CACHE_FLUSH_TIMER to 1 second to minimize the flush time:

```
HSGA> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=1
HSGA> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=1
```

7. Determine whether all data has been flushed from the cache module:

```
HSGA> SHOW THIS_CONTROLLER
```

The following text is only a portion of the resulting display:

```
Cache:
        256 megabyte write cache, version 0022
        Cache is GOOD
        No unflushed data in cache
        CACHE_FLUSH_TIMER=1 SECOND
```

Note: Repeat step 7 on both controllers (THIS_CONTROLLER and OTHER_CONTROLLER) until no unflushed data remains in either cache module memory.

8. Shut down both controllers:

```
HSGA> SHUTDOWN OTHER_CONTROLLER
HSGA> SHUTDOWN THIS_CONTROLLER
```

Note: After the controllers shut down, the **Reset** buttons and the first three LEDs on both controllers turn on (see Figure 38 on page 226). This could take several minutes, depending on the amount of data that needs to be flushed from the cache modules. Proceed only after both **Reset** buttons stop flashing and remain on.

9. Upgrade the software on both controllers:

Note: After step 9 is performed, the previous ACS version cannot be restored to this subsystem without performing the downgrade process, which should be performed only by HP authorized service personnel.

a. Remove the program card ESD cover from Controller A.
b. While pressing and holding the controller **Reset** button, eject the old program card.
c. After ejecting the program card, release the **Reset** button.
d. Repeat step a through step c for Controller B.

Note: In step e and step f, the simultaneous release of the **Reset** buttons is essential to ensure that both controllers are restarted and upgraded simultaneously.

e. Simultaneously press and hold the **Reset** button on both controllers, and insert a new program card into each controller.
f. Simultaneously release the **Reset** buttons. Both controllers restart.

Note: A controller restart can take as long as 60 seconds and is indicated by the temporary cycling of the port LEDs and a flashing **Reset** button. Disregard messages about misconfigured controllers or failover status.

g. Install a program card ESD cover on each controller.

Caution: Stop upgrading the initiator site controllers at this point and proceed to upgrade the target site controllers. Failure to upgrade the target site controllers at this point could cause the initiator and target site controllers to crash and prevent the host from accessing data stored in these subsystems.

The initiator site shutdown upgrade procedure continues on page 236 after the target site shutdown upgrade procedure.

Continue the shutdown upgrade procedure by executing the following steps on the target site controllers.

Target Site Shutdown Upgrade Procedure

Note: During the target site upgrade, one of the initiator site controllers could restart with an instance code of 0xE096980. This potential restart is expected; disregard the associated instance code.

1. From a host console, stop all host activity to the controllers and dismount the logical units in the subsystem.
2. Connect a PC or terminal to the maintenance port of Controller A at the target site.
3. Delete all snapshot units by performing the following steps:
   a. Identify all snapshot units:

      ```
      HSGA> SHOW UNITS FULL
      ```

   b. Record the configuration for each snapshot unit for restoration in step 11.
   c. Delete all snapshot units individually:

      ```
      HSGA> DELETE snapshot-unit-name
      ```

4. Verify that all snapshot units are deleted by issuing the following command:

   ```
   HSGA> SHOW UNITS FULL
   ```

Note: If any snapshot unit exists, repeat step 3.

5. Identify and record the current CACHE_FLUSH_TIMER value:

   ```
   HSGA> SHOW THIS_CONTROLLER
   ```

   The following text is only a portion of the resulting display:

   ```
   Cache:
           256 megabyte write cache, version 0022
           Cache is GOOD
           No unflushed data in cache
           CACHE_FLUSH_TIMER=DEFAULT (10 seconds)
   ```

Note: The CACHE_FLUSH_TIMER value is displayed in the caching parameters section. This parameter is modified during the procedure and must be restored in step 10.

6. Set the CACHE_FLUSH_TIMER to 1 second:

   ```
   HSGA> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=1
   HSGA> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=1
   ```

7. Determine whether all data has been flushed from the cache module by issuing the following command:

   ```
   HSGA> SHOW THIS_CONTROLLER
   ```

   The following text is only a portion of the resulting display:

```
Cache
        256 megabyte write cache, version 0022
        Cache is GOOD
        No unflushed data in cache
        CACHE_FLUSH_TIMER=1 SECOND
```

Note: Repeat this step on both controllers (THIS_CONTROLLER and OTHER_CONTROLLER) until no unflushed data remains in either cache module memory.

8. Shut down both controllers:

```
HSGA> SHUTDOWN OTHER_CONTROLLER
HSGA> SHUTDOWN THIS_CONTROLLER
```

Note: After the controllers shut down, the **Reset** buttons and the first three LEDs on both controllers turn on (see Figure 38 on page 226). This could take up to 15 minutes, depending on the amount of data that needs to be flushed from the cache modules. Proceed only after both **Reset** buttons stop flashing and remain on.

9. Upgrade the software on both controllers:

Note: After step 9 is performed, the previous ACS version cannot be restored to this subsystem without performing the downgrade process, which should be performed only by HP authorized service personnel.

a. Remove the program card ESD cover from Controller A.
b. While pressing and holding the controller **Reset** button, eject the old program card.
c. After ejecting the program card, release the **Reset** button.
d. Repeat step a through step c for Controller B.

Note: In step e and step f, the simultaneous release of the **Reset** buttons is essential to ensure that both controllers are restarted and upgraded simultaneously.

e. Simultaneously press and hold the **Reset** buttons on both controllers, and insert a new program card into each controller.
f. Simultaneously release the **Reset** buttons. Both controllers restart.

Note: A controller restart can take as long as 60 seconds and is indicated by the temporary cycling of the port LEDs and a flashing **Reset** button. Disregard messages about misconfigured controllers or failover status.

g. Install a program card ESD cover on each controller.

10. After the controllers restart, restore the CACHE_FLUSH_TIMER to the value recorded in step 5 on page 232:

```
HSGB> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=n
HSGB> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=n
```

11. Restore all snapshot units removed in step 3.
12. Mount the logical units on the host.
13. Disconnect the PC or terminal from the maintenance port of Controller A.

Completion of Initiator Site Shutdown Upgrade Procedure

1. After the controllers restart, restore the CACHE_FLUSH_TIMER to the value recorded in step 5 on page 232:

```
HSGB> SET THIS_CONTROLLER CACHE_FLUSH_TIMER=n
HSGB> SET OTHER_CONTROLLER CACHE_FLUSH_TIMER=n
```

2. Restore all snapshot units removed in step 3 on page 234.
3. Mount the logical units on the host.
4. Disconnect the PC or terminal from the maintenance port of Controller A.

This completes the shutdown upgrade to ACS Version 8.7P software.

Glossary

This glossary defines terms used in this guide or related to the Data Replication Manager. It is not a comprehensive glossary of computer terms.

ACS
An acronym for array controller software. *See* array controller software.

adapter
A hardware device that converts the protocol and hardware interface of one bus type to another without changing the function of either bus.

AL_PA
or
ALPA
An acronym for Arbitrated Loop Physical Address. A two-digit hexadecimal number that expresses a port's physical position on the loop. ALPA numbers are normally not assigned in sequence (that is, position 1 is not ALPA 1, and so on). A table in the Fibre Channel Standard equates the loop position to the default ALPA.

arbitrated loop
A Fibre Channel topology. The basic definition is a ring of ports where the transmit output of one port is attached to the receive input of the next. Each port has a unique loop address and it talks to other ports on the loop by arbitrating for loop access. Loop addresses are assigned via cooperative port intercommunication during loop initialization, which occurs any time the device configuration on the loop is physically changed. PLDA (private loop direct attach), the specific profile implemented by the controller, is a subset of arbitrated loop.

See also PL_DA or PLDA.

array controller
See controller.

array controller software (ACS)
Software that is contained on a removable PCMCIA program card that provides the operating environment for the array controller.

association sets
An association set is a group of remote copy sets that share common attributes. Members of an association set are configured to transition to the same state at the same time. An association set:

- Shares the same log unit
- Has its host access removed from all members when one member fails
- Keeps I/O order across all members
- Fails over to the alternate controller in the event of primary controller failure.

CLI commands available are `ADD ASSOCIATIONS` and `SET associations`.

asynchronous mode
A mode of operation of the remote copy set whereby the write operation provides command completion to the host after the data is safe on the initiating controller, and prior to the completion of the target command.

Asynchronous mode can provide faster response time, but the data on all members at any one point in time cannot be assumed to be identical.

See also synchronous mode.

ATM
Asynchronous Transfer Mode. ATM refers to a network or communications technology used in LANs and WANs to enable disparate traffic (data, voice, and video) to be carried over the same local or wide area network. ATM is the transfer mode of choice for broadband integrated services digital networks (BISDNs). ATM traffic carries information in fixed-size cells.

autospare
A controller feature that automatically replaces a failed disk drive with a working drive. The operator can enable the AUTOSPARE switch for the failedset, causing physically replaced disk drives to be automatically placed into the spareset. Data recovery is outside the scope of autosparing. Also called *autonewspare*.

B-series switches
Fibre Channel core and SAN switches made by Brocade and sold by HP.

bad block
A disk drive data block that contains a physical defect.

bad block replacement
A replacement routine that substitutes defect-free disk blocks for those found to have defects. This process takes place in the controller, transparent to the host.

BBR
See bad block replacement.

block
A stream of data stored on disk or tape media and transferred and error-checked as a unit. In a disk drive, a block is also called a sector (the smallest collection of consecutive bytes addressable on a disk drive). In HP integrated storage elements, a block contains 512 bytes of data, error codes, flags, and the block address header.

C-series switches
Switches made by Cisco.

cache
A fast, temporary storage buffer in a controller or computer.

cache memory
Portion of high-speed memory used as an intermediary between a data user and a larger amount of storage. The objective of designing cache into a system is to improve performance by placing the most frequently used data in the highest performance memory and close to the process needing that data.

CBR
An acronym for Constant Bit Rate, a category of ATM service. This category supports a constant (guaranteed) data rate. CBR supports applications that require a highly predictable transmission rate.

cascaded switch
As applied to the Data Replication Manager, the term cascaded switch identifies that the output of a switch is connected to the input of another switch, which then may in turn be connected to another switch or host or controller.

chunk
A block of data written by the host.

See also block, chunk size.

chunk size
The number of data blocks, assigned by a system administrator, that are written to the primary RAIDset or stripeset member before the remaining data blocks are written to the next RAIDset or stripeset member. Nondefault chunk size values must be exactly divisible by 8.

CLI
An acronym for command line interface. The CLI is the configuration interface to operate the controller software.

clone
A utility that physically duplicates data on any unpartitioned single-disk unit, stripeset, mirrorset, or striped mirrorset.

command line interface
See CLI.

connection
As applied to the Data Replication Manager, this refers to a connection between two-end Fibre Channel ports. An example would be the connection between a host bus adapter (by way of the Fibre Channel switches) and the HSG80 controller.

CLI commands available on the HSG80 are `ADD CONNECTIONS, SET connection_name`.

See also link.

container
1. Any entity that is capable of storing data, whether it is a physical device or a group of physical devices.
2. A virtual internal controller structure representing either a single disk or a group of disk drives linked as a storageset. Examples of storageset containers that the controller uses to create units include stripesets and mirrorsets.

controller
A hardware device that uses software to facilitate communications between a host and one or more storage devices organized in an array. The HS-series *StorageWorks*™ family of controllers are all array controllers.

copying member
In a mirrorset, a copying member is a container introduced to the mirrorset after the mirrorset has already been in use. None of the blocks can be guaranteed to be the same as other members of the mirrorset. Therefore the *copying* member is made the same by copying all the data from a *normal* member. This is in contrast to *normalization*, where all blocks written since creation are known to be the same.

When all of the blocks on the copying member are the same as those on the normal member, the copying member becomes a normal member. Until it becomes a normal member, the copying member contains undefined data and is not useful for any purpose.

DataSafe
Also known as firewall for Microsoft Windows 2000 and NT. This pre-tested configuration uses specific hardware, Data Replication Manager software, and installation practices to protect operations from hardware or software outages. The solution includes No Single Point of Failure (NSPOF) functionality.

default gateway
The default path that a computer or router uses to forward and route data between two or more networks having different protocols.

device
See node, peripheral device.

disaster tolerance
As applied to DRM, disaster tolerance provides the ability for rapid recovery of user data from a remote location when a significant event or a disaster occurs at the primary computing site.

See also remote copy sets, DT.

DT
An acronym for disaster tolerance.

See disaster tolerance.

dual-redundant configuration
A storage subsystem configuration consisting of two active controllers operating as a single controller. If one controller fails, the other controller assumes control of the failing controller's devices.

See also failover, failback.

ECB
An acronym for external cache battery.

See external cache battery.

EMU
Environmental Monitoring Unit. A device that provides increased protection against catastrophic failures. Some subsystem enclosures include an EMU, which works with the controller to detect conditions such as failed power supplies, failed blowers, elevated temperatures, and external air sense faults. The EMU also controls certain rack hardware, including alarms, fan speeds, and certain chips.

environmental monitoring unit
A piece of hardware that provides increased protection against catastrophic failures. Some subsystem enclosures include an EMU, which works with the controller to detect conditions such as failed power supplies, failed blowers, elevated temperatures, and external air sense faults. The EMU also controls certain rack hardware, including DOC chips, alarms, and fan speeds.

external cache battery
The unit that supplies backup power to the cache module in the event the primary power source fails or is interrupted.

E1
The standard European carrier for transmission at 2.048 Mbit/sec.

E2
The standard European carrier for transmission at 8.192 Mbit/sec.

E3
The standard European carrier for transmission at 34.368 Mbit/sec.

E4
The standard European carrier for transmission at 139.264 Mbit/sec.

E5
The standard European carrier for transmission at 565 Mbit/sec.

F_port
A port in a fabric where an N_Port or NL_Port may attach.

fabric
A network of Fibre Channel switches or hubs and other devices.

failback
The process of restoring data access to the newly restored controller in a dual-redundant controller configuration. The failback method (full copy or fast failback) is determined by the enabling of the Logging or Failsafe switches, the selected mode of operation (synchronous or asynchronous), and whether the failover is planned or unplanned.

See also failover, dual-redundant configuration.

failedset
A group of disk drives that have been removed from RAIDsets due to a failure or a manual action. Disk drives in the failedset should be considered defective and should be tested and repaired before being placed back into the spareset or back in their original locations.

failover
The process that takes place when storage processing is moved from one pair of controllers at one site to another pair at another site. Failover continues until the processing is failed back to the originator site.

The CLI command is: `SITE_FAILOVER`

See also failback, dual-redundant configuration, planned failover.

failsafe locked
The failsafe error mode can be enabled by the user to fail any write I/O whenever the target is inaccessible or the initiator unit fails. When either of these conditions occurs, the remote copy set goes into the inoperative (offline) state and the failsafe error mode is *failsafe locked*.

The CLI command `SET` *`remote-copy-set-name`* `ERROR_MODE=FAILSAFE` enables this error mode.

fast failback
A term representing the synchronization of the initiator site with the target during a planned failback from the target back to the initiator.

The write operations are logged to the target site write history log, and during the fast failback, the initiator site is updated from the write history log.

See also mini-merge, unplanned failover, planned failover, write history logging.

FC–AL
or
FCAL
An acronym for Fibre Channel Arbitrated Loop. FC-AL is the overall Fibre Channel topology whose basic definition is a ring of ports where the transmit outputs of one port are attached to the receive input of the next. Not supported by DRM.

FCC
An acronym for the Federal Communications Commission. The federal agency responsible for establishing standards and approving electronic devices within the United States.

FCC Class A
This certification label appears on electronic devices that can only be used in a commercial environment within the United States.

FCC Class B
This certification label appears on electronic devices that can be used in either a home or a commercial environment within the United States.

FCP
An acronym for Fibre Channel Protocol. The mapping of SCSI-3 operations to Fibre Channel.

FDDI
An acronym for Fiber Distributed Data Interface. An ANSI standard for 100 megabaud transmission over fiber optic cable.

FD SCSI
The fast, narrow, differential SCSI bus with an 8-bit data transfer rate of 10 MB/s.

See FWD SCSI and SCSI. More information is available from http://www.t10.org.

fiber
An optical strand used in fiber optic cable. Spelled fibre when used in "Fibre Channel" protocol.

See also fiber optic cable, Fibre Channel.

fiber optic cable
A transmission medium designed to transmit digital signals in the form of pulses of light. Fiber optic cable is noted for its properties of electrical isolation and resistance to electrostatic contamination. Available in three sizes: 50-micron multimode, 9-micron single-mode, and, in older installations, 62.5-micron multimode (not recommended for new installations).

Fibre Channel
An ANSI standard name given to a low-level protocol for a type of serial transmission. The Fibre Channel specifications define the physical link, the low level protocol, and all other pertinent characteristics.

FL_port
A port in a fabric where N_port or an NL_port may be connected.

See N_port, NL_port, F_Port.

See also fabric.

firewall
A generic term used to describe a limited DRM configuration consisting of only two switches. The maximum distance between any two components is 500 meters due to the short range GBICs.

See also DataSafe.

frame
A frame is the basic unit of communication using the Fibre Channel protocol. Each frame consists of a payload encapsulated in control information. The initiator breaks up the exchange into one or more sequences, which in turn are broken into one or more frames. The responder recombines the frames into sequences and exchanges.

See also initiator.

FWD SCSI
Acronym for fast, wide, differential (FWD) Small Computer System Interface (SCSI) bus with a 16-bit data transfer rate of up to 20 MB/sec.

See also FD SCSI and SCSI.

GBIC
An acronym for gigabit interface converter. The hardware devices inserted into the ports of the Fibre Channel switch that hold the Fibre Channel cables. A GBIC converts fiber optic cable connections to Fibre Channel switch connections.

GBICs are available in three types: shortwave, longwave, and very long distance. Shortwave is limited to 50-micron multimode cable and 500 meters. Longwave uses 9-micron single-mode cable and is limited to a maximum distance of 10 kilometers. Very long distance also uses 9-micron low-loss cable and may extend to 100 kilometers.

GLM
Gigabit Link Module, used in short-wave multimode fiber only. GLMs, as a function of GBIC, are used in Fibre Channel long-distance applications. As applied to the Data Replication Manager, the GLMs provide the ability to increase the fiber optic cable transmission distances from 10 km to 70 km.

hard address
The AL_PA or ALPA which an NL_port attempts to acquire during loop initialization. Not used by DRM.

heterogeneous host support
Also called noncooperating host support. The ability to share storage between two similar (or dissimilar) hosts by way of storage partitioning.

HIPPI–FC
An acronym for the high-performance parallel interface (HIPPI) over the Fibre Channel. HIPPI is a media-level, point-to-point, 12-channel, full-duplex, electrical/optical interface. Not supported by DRM. See http://www.t11.org for more information.

hop
The definition of an interswitch connection. For example, there is one hop between two cascaded switches.

ISL
Intersite link or interswitch link. The abbreviation is context sensitive.

See also multiple intersite links.

initiator

1. A SCSI device that requests an I/O process to be performed by another SCSI device, namely, the SCSI target. The controller is the initiator on the device bus.
2. For subsystems using the disaster tolerant Data Replication Manager solution, the initiator is the site that is the primary source of information. In the event of a system outage, the data would be recovered from the target system.

See also target.

IP address
An abbreviation for Internet Protocol Address. The IP address is a number that is used as the address specifying a particular computer connected to the Internet.

L_port
A node or fabric port capable of performing arbitrated loop functions and protocols. NL_port and FL_Port are loop-capable ports.

latency
The amount of time required for a transmission to reach its destination.

LBN
An acronym for logical block number.

See logical block number.

link
A physical connection between two adjacent Fibre Channel ports, consisting of a transmit fiber and a receive fiber. An example would be the connection between the Fibre Channel switch port and the HSG80 controller.

See also connection.

local terminal
A terminal plugged into the EIA-423 maintenance port on the front bezel of the HS array controller. Also called a maintenance terminal.

Logical block number
A volume-relative address of a block on a mass storage device. The blocks that form the volume are labeled sequentially starting with LBN 0.

logical unit
A physical or virtual device addressable through a target ID number. The logical unit numbers (LUNs) use their target's bus connection to communicate on the SCSI bus.

See logical unit number.

logical unit number
A value that identifies a specific logical unit belonging to a SCSI target ID number. A number associated with a physical device unit during a task's I/O operations. Each task in the system must establish its own correspondence between logical unit numbers and physical devices.

LOG_UNIT
A CLI command switch that (when enabled) assigns a single, dedicated log unit for a particular association set. The association set members must all be in the NORMAL error mode (not failsafe).

See also write history logging.

long distance mirroring
Also known as peer-to-peer remote copy.

See also remote copy sets.

loop
See arbitrated loop.

loop_ID
A seven-bit value numbered contiguously from zero to 126-decimal, which represents the 127 legal AL_PA or ALPA values on a loop (not all of the 256 hex values are allowed as AL_PA values per FC-AL).

loop tenancy
The period of time between the following two events: when a port wins loop arbitration and when the port returns to a monitoring state.

LUN
An acronym for logical unit number.

See logical unit number.

M-series switches
Fibre Channel Director and Edge switches made by McDATA and sold by HP.

mini-merge
As applied to the Data Replication Manager, a term representing the data transfers to be made from the write history log when the target becomes available after having been unavailable. This happens when both links or both target controllers have gone down. The transfers that would have been made are instead logged into the association set's assigned log unit to wait until the remote copy set subsystem comes back online.

See fast failback, write history logging.

mirroring
The act of continuously creating an exact physical copy or image of data.

mirrorset
1. A group of storage devices organized as duplicate copies of each other. Mirrorsets provide the highest level of data availability at the highest cost. Another name for RAID 1. Also called mirrored units or mirrored virtual disks.
2. Two or more physical disks configured to present one highly reliable virtual unit to the host.
3. A virtual disk drive consisting of multiple physical disk drives, each of which contains a complete and independent copy of the entire virtual disk's data.

multiple intersite links
Each intersite link (ILS) is a fiber link between two switches. As applied to Data Replication Manager, increasing bandwidth between switches is handled by adding connections between the switches, to a maximum of two connections.

N_port
A port attached to a node for use with point-to-point topology or fabric topology.

See point-to-point connection.

network
In data communication, a configuration in which two or more terminals or devices are connected to enable information transfer.

NL_port
A port attached to a node for use in all three Fibre Channel topologies: point-to-point, arbitrated loop, and switched fabric.

node

1. In data communications, the point at which one or more functional units connect transmission lines.
2. In Fibre Channel, a device that has at least one N_port or NL_port.

Non-L_port
A node or fabric port that is not capable of performing the arbitrated loop functions and protocols. N_Ports and F_Ports are loop-capable ports.

nonparticipating mode
A mode within an L_Port that inhibits the port from participating in loop activities. L_Ports in this mode continue to retransmit received transmission words but are not permitted to arbitrate or originate frames. An L_Port in nonparticipating mode may or may not have an AL_PA.

See also participating mode.

non-RCS LUN
As applied to Data Replication Manager, a logical unit number (LUN) value that identifies a physical device unit which exists at one of the two sites and does not have a mirror copy at the other site.

See also remote copy sets, LUN.

normal member
A mirrorset member that, block for block, contains exactly the same data as that on the other members within the mirrorset. Read requests from the host are always satisfied by normal members.

normalizing
A state in which, block for block, data written by the host to a mirrorset member is consistent with the data on other normal and normalizing members. The normalizing state exists only after a mirrorset is initialized. Therefore, no customer data is on the mirrorset.

normalizing member
A mirrorset member whose contents are the same as all other normal and normalizing members for data that has been written since the mirrorset was created or since lost cache data was cleared. A normalizing member is created by a normal member when either all of the normal members fail or all of the normal members are removed from the mirrorset.

See also copying member.

OC-3
An acronym for the optical carrier that provides high-speed bandwidth at 155.3 megabits per second.

other controller
The controller in a dual-redundant pair that is not connected to the controller serving your current CLI session with a local terminal.

See also this controller, local terminal.

participating mode
A mode within an L_port that allows the port to participate in loop activities. A port must have a valid AL_PA or ALPA to be in participating mode.

PCM
An acronym for Polycenter Console Manager.

PCMCIA
An acronym for Personal Computer Memory Card Industry Association. An international association formed to promote a common standard for PC card-based peripherals to be plugged into notebook computers. A PCMCIA card, sometimes called a PC Card, is about the size of a credit card. It is used in the HSJ80 to load the controller software.

See also program card, ACS.

PCR
An acronym for peak cell rate, the maximum transmission speed of a virtual connection. PCR is a required parameter for the CBR service category.

peer-to-peer remote copy
See remote copy sets.

peripheral device
Any unit, distinct from the CPU and physical memory, that can provide the system with input or accept any output from it. Terminals, printers, tape drives, and disks are peripheral devices.

planned failover
As applied to the Data Replication Manager, an orderly shutdown of the initiator site applications and controllers for installation of new hardware, updating the software, and so on. The host applications are quiesced and all write operations are permitted to complete before the shutdown. The controllers must be in synchronous operation mode before starting a planned failover.

See also synchronous mode, unplanned failover.

PL_DA
or
PLDA
An acronym for Private Loop Direct Attach. PLDA is a Fibre Channel profile, a proper subset of arbitrated loop. The PLDA profile (part of the Fibre Channel Standard), defines a specific way to implement arbitrated loop topology. Not supported by DRM.

See arbitrated loop.

point-to-point connection
A network configuration in which a connection is established between two, and only two, terminal installations. The connection may include switching facilities.

See N_port.

port

- In general terms, a port is:
  - A logical channel in a communications system.
  - The hardware and software used to connect a host controller to a communications bus, such as a SCSI bus or serial bus.
- Regarding the controller, the port is:
  - The logical route for data in and out of a controller that can contain one or more channels, all of which contain the same type of data.
  - The hardware and software that connect a controller to a SCSI device.

port_name
A 64-bit unique identifier assigned to each Fibre Channel port. The port_name is communicated during the logon and port discovery process.

preferred address
The AL_PA which an NL_Port attempts to acquire first during initialization.

private NL_port
An NL_Port which does not attempt login with the fabric and only communicates with NL_Ports on the same loop. Not used by DRM.

public NL_port
An NL_port that attempts login with the fabric and can observe the rules of either public or private loop behavior. A public NL_Port may communicate with both private and public NL_Ports. Not used by DRM.

program card
The PCMCIA card containing the controller's operating software.

See also PCMCIA.

PTL
An acronym for Port-Target-LUN. The controller's method of locating a device on the controller device bus:

- P designates the port (1 through 6)
- T designates the target ID of the device (1 through 6 in a nonredundant configuration, or 0 through 5 in a dual-redundant configuration)
- L designates the LUN of the devices (0 through 7).

PVA module
An abbreviation for Power Verification and Addressing module. The Ultra SCSI RAID enclosure assembly whose primary functions are to: (1) allow the user to select the enclosure Ultra SCSI bus ID; (2) enable the user to place the subsystem in a standby condition and return it to an operational status; and (3) in conjunction with the associated EMU, ensures that the major Ultra SCSI elements are functioning properly and notifies the user and the controller of error or fault conditions.

PVC
An acronym for Permanent Virtual Circuit. PVC is a logical connection manually defined by the network administrator. The PVC is created by specifying the VPI and VCI.

quiesce
To make a bus inactive or dormant. In a DRM environment, quiesce means to shut down or freeze applications such that all pending I/O is completed and no new I/O is initiated by the application until a thaw or unquiesce command is issued. During a device warm swap, the SCSI bus must quiesce.

See also planned failover.

QoS
An acronym for Quality of Service in an ATM network. Each virtual connection in an ATM network is set to a service category. The performance of the connection is measured by the established QoS parameters (outlined by the ATM Forum).

Performance issues include data rate, cell loss rate, cell delay, and delay variation (jitter).

Categories of ATM service are:

- Constant Bit Rate (CBR)
- Variable Bit Rate-Real Time (VBR-RT)
- Variable Bit Rate-Non-Real Time (VBR-NRT)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)

See also ATM.

RCS
See remote copy sets.

redundancy
The provision of multiple interchangeable components to perform a single function in order to cope with failures and errors. A RAIDset is considered to be redundant when user data is recorded directly to one member, and all of the other members and associated parity also are recorded. If a member is missing from the RAIDset, its data can be regenerated as needed, but the RAIDset is no longer redundant until the missing member is replaced and reconstructed.

remote copy sets
A feature that allows data to be copied (mirrored) from the originating site (initiator) to a remote site (target). The result is a mirror copy of the data (remote copy set) at two disparate sites. Used in disaster tolerance (DT) applications such as the Data Replication Manager.

CLI commands available are: `ADD REMOTE_COPY_SETS`, `SET remote-copy-set-name`, `SET controller REMOTE_COPY`.

See also disaster tolerance, non-RCS LUN.

remote copy set metadata
Remote copy set metadata describes the remote copy set membership and state. To assist with site failover, this metadata is located in the mirrored write-back cache on the controller where each member resides. Backup copies of the metadata reside in the controller NVRAM at each site. Only the initiator modifies the metadata and ensures all copies are subsequently updated.

replacement policy
The policy specified by a CLI command switch (`SET FAILEDSET` command) indicating whether a failed disk from a mirrorset or RAIDset is to be automatically replaced with a disk from the spareset. The two switch choices are `AUTOSPARE` and `NOAUTOSPARE`.

SCSI
An acronym for Small Computer System Interface:

1. An American National Standards Institute (ANSI) interface standard defining the physical and electrical parameters of a parallel I/O bus used to connect initiators to devices.
2. A processor-independent standard protocol for system-level interfacing between a computer and intelligent devices, including hard drives, floppy disks, CD-ROMs, printers, scanners, and others.

Refer to http://www.t10.org for more information.

SCSI device

1. A host computer adapter, a peripheral controller, or an intelligent peripheral that can be attached to the SCSI bus.
2. Any physical unit that can communicate on a SCSI bus.

SCSI device ID number

A bit-significant representation of the SCSI address referring to one of the signal lines, numbered 0 through 7 for an 8-bit bus, or 0 through 15 for a 16-bit bus.

SCSI ID number

The representation of the SCSI address that refers to one of the signal lines numbered 0 through 15.

snapshot

A snapshot unit is one that reflects the contents of another unit at a particular point in time. It is a virtual copy and not a physical copy of the source device at a point in time.

See also unit.

storage array

An integrated set of storage devices. Storage arrays can be manipulated as one unit.

storage unit

The general term that refers to storagesets, single-disk units, and all other storage devices that are installed in a subsystem and accessed by the host. A storage unit can be any entity that is capable of storing data, whether it is a physical device or a group of physical devices.

storageset

1. A group of devices configured with RAID techniques to operate as a single container.
2. Any collection of containers, such as stripesets, mirrorsets, striped mirrorsets, JBODs, and RAIDsets.

subnet mask

Also known as address mask. A subnet is an IP network that can be reached through a single IP address. All the members of the subnet share the mask value. Members of the subnet can then be referenced more easily. A subnetwork is a network that is part of another network, connected through a gateway, bridge, or router.

surviving controller

The controller in a dual-redundant configuration pair that serves its companion's devices when the companion controller fails.

SWCC

An acronym for StorageWorks Command Console.

synchronous mode

A mode of operation of the remote copy set whereby the data is written simultaneously to the cache of the initiator subsystem and the cache of the target subsystem. The I/O completion status is not sent until all members of the remote copy set are updated.

See also asynchronous mode.

target

A SCSI device that performs an operation requested by another SCSI device, namely the SCSI initiator. The target number is determined by the device's address on its SCSI bus.

For subsystems using the disaster-tolerant Data Replication Manager solution, data processing occurs at the initiator site and the data is replicated or mirrored to the target site. In the event of a system outage, the data is recovered from the target system.

See also initiator.

this controller
The controller that is serving the current CLI session through a local or remote terminal.

See also other controller.

T1
The standard North American carrier for transmission at 1.544 Mbit/sec.

T2
The standard North American carrier for transmission at 6.176 Mbit/sec.

T3
The standard North American carrier for transmission at 44.736 Mbit/sec.

UBR
An acronym for unspecified bit rate. The UBR is a category of ATM service that supports connections that have no specified performance requirements.

ULP
An acronym for Upper Layer Protocol.

ULP process
A function executing within a Fibre Channel node which conforms to the Upper Layer Protocol (ULP) requirements when interacting with other ULP processes.

UltraNet Wizard
Another term for the Fibre Channel-to-ATM Configuration Wizard. This wizard is an UltraNet application that allows the designation of the default configuration settings for Fibre-Channel-ATM on the Open Systems Gateway.

unit
A container made accessible to a host. A unit may be created from a single disk drive or tape drive. A unit may also be created from a more complex container, such as a RAIDset. The controller supports a maximum of eight units on each target.

index

A

add associations command 39, 116
add mirrorset command 115
add remote copy set command 112, 113
add snapshot units command 220
add unit command 69, 107, 116
AIX
  configuring SWCC agent at initiator site 133
  configuring SWCC agent at target site 90
  connecting host to SAN at initiator site 132
  connecting host to SAN at target site 88
  disabling access to hosts at target site 89
  enabling access to hosts at initiator site 133
  installing HBAs at initiator site 126
  installing HBAs at target site 82
  installing platform kit at target site 83, 126
  installing Secure Path Fibre Channel HBA device driver at target site 83, 126
  renaming host connections at initiator site 132
  renaming host connections at target site 88
  setting up at initiator site 126
  setting up at target site 82
  updating switch zones at initiator site 132
  updating switch zones at target site 89
  verifying disks at initiator site 133
  verifying disks at target site 89
aliCreate command 201, 202
assigning World Wide Name 64
association sets
  characteristics of 37
  creating at initiator site 115, 116
  definition 37
  FAIL_ALL switch 38
  location on initiator controller pair 38
  LOG_UNIT switch 41
  ORDER_ALL switch 42
  re-creation upon site failover 39
asynchronous operation mode 34
audience 14
authorized reseller, HP 18

B

BA370 enclosure 21

C

cabling
  between controllers and Fibre Channel switches 110
  from initiator to target site 111
  the initiator site 109 to 110
  the target site 71 to 73
cascaded switches 52
  configurations 53
cfgAdd command 205
cfgCreate command 196, 197
cfgEnable command 196, 197, 205, 206, 208
cfgShow command 205, 207
changing SCSI version 49
  rolling upgrade 52
  static upgrade 49
clone 217
clone utility 217
clone utility, backup 217
cloning and snapshot comparison 215
cloning defined 215
cluster server, installing for Windows 144
cluster services, installing for NetWare 144
commands
  add associations 39, 116
  add mirrorset 115
  add remote copy set 112, 113
  add snapshot units 220
  add unit 69, 107, 116
  aliCreate 201, 202
  cfgAdd 205
  cfgCreate 196, 197
  cfgEnable 196, 197, 205, 206, 208
  cfgShow 205, 207

delete 220, 224, 228, 232
initialize 115
rename 76, 120, 122, 136, 139, 142
restart controller 67, 70, 105, 108
scan for new devices 140
set alloclass 65
set cache flush timer 225
set controller identifier 65
set controller mirrored cache 66, 104
set controller node 102
set controller port topology 67, 105
set controller prompt 104
set controller remote copy 68, 106
set disable 89
set disable access path 69, 107, 116
set enable access path 113, 120, 133, 140
set error mode 114
set fail all 118
set identifier 103
set log unit 117
set maximum cached transfer size 69
set multibus failover copy 103
set nowriteback cache 116, 225, 229
set operating system to AIX 89
set operating system to NetWare 95, 139
set operating system to OpenVMS 120
set operating system to Solaris 98, 142
set operating system to Tru64 UNIX 79, 122
set operating system to Windows 92, 136
set order all 118
set preferred path 70, 108
set SCSI mode 103
set unit identifier 69, 107
set writeback cache 231
show associations 212
show connections 76, 78, 79, 89, 212
show remote 179
show remote copy 212
show units 116
shutdown controller 226, 232, 235
snapshot 220
switch version 167
switchShow 168, 169, 171, 173
zoneAdd 208
zoneCreate 196, 204
components, software required for disaster tolerance 30
configurations
heterogeneous 197
homogeneous 185
multiple intersite links 55
configuring
controllers at initiator site 100 to 106
controllers at target site 62 to 68
host at initiator site 118 to 144
host at target site 74 to 100
storage at initiator site 107 to 109
storage at target site 69 to 71
connections
defined 48
host-to-switch 48
switch-to-controller 48
controller replacement 181 to ??
controllers, configuring for multiple-bus failover 65
conventions
document 15
equipment symbols 16
text symbols 15
creating zone names 196, 204

D

data security 184
delete command 220, 224, 228, 232
document
conventions 15
related documentation 14
DRM
basic configuration 58
command line interface (CLI) to 60
components 25
enabling at initiator site 106
operating restrictions 58

E

EMA12000 rack 21, 27
EMA16000 rack 21
enclosure, BA370 21
environmental monitoring unit (EMU) 24
equipment symbols 16
error mode
failsafe 37
normal switch setting for 37
switch 37
ESA12000 rack 21, 27
Ethernet 46

F

fabric topology, setting 67
failback 43
failover
planned 42
unplanned 43
failsafe, setting at initiator site 114
fiber optic cable
connecting between target controllers and switches 71
host-to-switch connections 48

multi-mode 27
setting up 47
single-mode 27
switch-to-controller connections 48
Fibre Channel
installing software for Windows at initiator site 134
installing software for Windows at target site 90
setting up switch 46
switch-to-controller connection 48
fully-redundant power 27

G

GBIC
fiber optic cable for 48
inserting short wave 72
long wave or very long distance 73, 111
short-wave 27, 110
getting help 17

H

hardware, required components 21
HBAs
installing driver for NetWare at initiator site 137
installing driver for NetWare at target site 93
installing driver for Tru64 UNIX at initiator site 121
installing driver for Tru64 UNIX at target site 77
installing driver for Windows at initiator site 134
installing driver for Windows at target site 90
installing for AIX at initiator site 126
installing for AIX at target site 82
installing for NetWare at initiator site 137
installing for NetWare at target site 93
installing for OpenVMS at initiator site 118
installing for OpenVMS at target site 74
installing for Solaris at initiator site 141
installing for Solaris at target site 96
installing for Tru64 UNIX at initiator site 121
installing for Tru64 UNIX at target site 77
installing for Windows at initiator site 134
installing for Windows at target site 90
overview 27
requirements 46
World Wide Name 62, 92
help, obtaining 17
heterogeneous configuration 197
homogeneous configuration 185
hop rules 52
host connections, limit of 96 184
hosts
host-to-switch connection 48
preparation 46
HP
authorized reseller 18
storage web site 17
technical support 17

I

initialize command 115
initiator site
assigning write history log units at 116
cabling of 109
changing prompts at 104
configuring controllers 100 to 106
configuring storage at 107 to 109
configuring SWCC agent for AIX 133
configuring SWCC agent for Solaris 144
configuring the host at 118 to 144
connecting host to SAN for AIX 132
connecting host to SAN for NetWare 138
connecting host to SAN for OpenVMS 119
connecting host to SAN for Solaris 141
connecting host to SAN for Tru64 UNIX 121
connecting host to SAN for Windows 135
creating association sets at 115, 116
creating remote copy sets at 112
creating storage units 107
creating switch zones at 112
creating write history log units at 115
enabling access to hosts for AIX 133
enabling access to hosts for NetWare 140
enabling access to hosts for OpenVMS 120
enabling access to hosts for Solaris 143
enabling access to hosts for Tru64 UNIX 123
installing Fibre Channel software for Windows 134
installing HBA driver for NetWare 137
installing HBA driver for Tru64 UNIX 121
installing HBA driver for Windows 134
installing HBAs for AIX 126
installing HBAs for NetWare 137
installing HBAs for OpenVMS 118
installing HBAs for Solaris 141
installing HBAs for Tru64 UNIX 121
installing HBAs for Windows 134
installing multipath software for Windows 134
installing Secure Path agent for NetWare 137
installing Secure Path for Solaris 143
installing Secure Path manager for NetWare 138
installing Solaris platform kit 141
installing SWCC for NetWare 138
installing SWCC for OpenVMS 118
installing SWCC for Tru64 UNIX 121
installing SWCC for Windows 135
renaming host connections for AIX 132
renaming host connections for NetWare 139
renaming host connections for OpenVMS 119
renaming host connections for Solaris 142
renaming host connections for Tru64 UNIX 122

renaming host connections for Windows 135
reverifying disks for Solaris 144
rolling upgrade procedure 224
setting failsafe at 114
setting up AIX at 126
setting up NetWare at 137
setting up OpenVMS at 118
setting up Solaris at 141
setting up Tru64 UNIX at 121
setting up Windows at 134
shutdown upgrade procedure 231
Tru64 UNIX multipath software support 121
updating switch zones for AIX 132
updating switch zones for NetWare 140
updating switch zones for OpenVMS 120
updating switch zones for Solaris 143
updating switch zones for Tru64 UNIX 123
updating switch zones for Windows 136
verifying disks for AIX 133
verifying disks for Solaris 143
intersite links
multiple 55

L

LUNs
configuring at target site 69
maximum number of non-RCS 59

M

MA8000 modular configuration 27
mirrored write-back cache 66
multi-mode fiber optic cable 27
multipath software
installing for Windows at initiator site 134
installing for Windows at target site 91
support for Tru64 UNIX at target site 78
multiple bus failover 65, 166
multiple e-port connectivity software option 55
multiple intersite links 55

N

NetWare
connecting host to SAN at initiator site 138
connecting host to SAN at target site 94
enabling access to hosts at initiator site 140
installing cluster services 144
installing HBA driver at initiator site 137
installing HBA driver at target site 93
installing HBAs at initiator site 137
installing HBAs at target site 93
installing Secure Path agent at initiator site 137
installing Secure Path agent at target site 93
installing Secure Path manager at initiator site 138
installing Secure Path manager at target site 94
installing SWCC at initiator site 138
installing SWCC at target site 94
renaming host connections at initiator site 139
renaming host connections at target site 95
setting up at initiator site 137
setting up at target site 93
updating switch zones at initiator site 140
updating switch zones at target site 96
non-remote copy set LUNS, maximum number 59
non-remote copy sets 34

O

OpenVMS
connecting host to SAN at initiator site 119
connecting host to SAN at target site 75
enabling access to hosts at initiator site 120
installing HBAs at initiator site 118
installing HBAs at target site 74
installing SWCC at initiator site 118
installing SWCC at target site 75
renaming host connections at initiator site 119
renaming host connections at target site 75
setting up at initiator site 118
setting up at target site 74
updating switch zones at initiator site 120
updating switch zones at target site 77
operation modes
asynchronous 34
considerations when designing 35
synchronous 34
outstanding I/O settings
asynchronous 36
default 35
high outstanding I/O values 36
low outstanding I/O values 36
outstanding write operations 36
synchronous 36

P

parameters for add snapshot unit command 220
peer-to-peer remote copy function 34
planned failover 42
power distribution unit (PDU) 27, 62
power, fully-redundant 27
prompts
changing at initiator site 104
changing at target site 66

R

RA8000 rack 27
rack stability, warning 17
racks

EMA12000 27
EMA16000 21
ESA12000 21, 27
RA8000 27
related documentation 14
remote copy function, peer-to-peer 34
remote copy sets
creating at initiator site 112
overview 34
resume switch 37
suspend switch 36
rename command 76, 120, 122, 136, 139, 142
replicating storage units, cloning data for backup 217
resource partitioning 184
restart controller command 67, 70, 105, 108
restrictions
Management Appliance 31
StorageWorks Command Console 31
rolling upgrade procedure 224 to 231

S

scan for new devices command 140
SCSI version
changing from SCSI-2 to SCSI-3 49
Secure Path
installing agent for NetWare at initiator site 137
installing agent for NetWare at target site 93
installing Fibre Channel HBA device driver for AIX at target site 83, 126
installing for Solaris at initiator site 143
installing for Solaris at target site 99
installing manager for NetWare at initiator site 138
installing manager for NetWare at target site 94
overview 30
set alloclass command 65
set cache flush timer command 225
set controller identifier command 65
set controller mirrored cache command 66, 104
set controller node command 102
set controller port topology command 67, 105
set controller prompt command 104
set controller remote copy command 68, 106
set disable access path command 69, 107, 116
set disable command 89
set enable access path command 113, 120, 133, 140
set error mode command 114
set fail all command 118
set identifier command 103
set log unit command 117
set maximum cached transfer size command 69
set multibus failover copy command 103
set nowriteback cache command 116, 225, 229
set operating system to AIX command 89
set operating system to NetWare command 95, 139
set operating system to OpenVMS command 120
set operating system to Solaris command 98, 142
set operating system to Tru64 UNIX command 79, 122
set operating system to Windows command 92, 136
set order all command 118
set preferred path command 70, 108
set SCSI mode command 103
set SCSI-3 mode 65
set unit identifier command 69, 107
set writeback command 231
short-wave GBIC 110
show associations command 212
show commands, issuing 212
show connections command 76, 78, 79, 89, 212
show remote command 179
show remote copy command 212
show units command 116
shutdown controller command 226, 232, 235
shutdown upgrade procedure 231 to 236
single-mode fiber optic cable 27
site preparation 46
snapshot
command 220
defined 215
unit 219, 220
software components required for disaster tolerance 30
Solaris
configuring SWCC agent at initiator site 144
configuring SWCC agent at target site 99
connecting host to SAN at initiator site 141
connecting host to SAN at target site 97
disabling access to hosts at target site 100
enabling access to hosts at initiator site 143
enabling access to hosts at target site 99
installing HBAs at initiator site 141
installing HBAs at target site 96
installing platform kit at initiator site 141
installing platform kit at target site 97
installing Secure Path at initiator site 143
installing Secure Path at target site 99
renaming host connections at initiator site 142
renaming host connections at target site 98
reverifying disks at initiator site 144
reverifying disks at target site 99
setting up at initiator site 141
setting up at target site 96
updating switch zones at initiator site 143
updating switch zones at target site 98
verifying disks at initiator site 143
verifying disks at target site 99

source unit 220
storage building block (SBB) 24
storage units
  creating at initiator site 107
  creating at target site 69
StorageWorks Command Console
  overview 31
SWCC
  configuring agent for AIX at initiator site 133
  configuring agent for AIX at target site 90
  configuring agent for Solaris at initiator site 144
  configuring agent for Solaris at target site 99
  installing for NetWare at initiator site 138
  installing for NetWare at target site 94
  installing for OpenVMS at initiator site 118
  installing for OpenVMS at target site 75
  installing for Tru64 UNIX at initiator site 121
  installing for Tru64 UNIX at target site 78
  installing for Windows at initiator site 135
  installing for Windows at target site 91
  overview 31
switch
  error mode 37
  version command 167
switch zones
  configuration variations 184
  creating at initiator site 112
  creating at target site 74
  updating for AIX at initiator site 132
  updating for AIX at target site 89
  updating for NetWare at initiator site 140
  updating for NetWare at target site 96
  updating for OpenVMS at initiator site 120
  updating for OpenVMS at target site 77
  updating for Solaris at initiator site 143
  updating for Solaris at target site 98
  updating for Tru64 UNIX at initiator site 123
  updating for Tru64 UNIX at target site 79
  updating for Windows at initiator site 136
  updating for Windows at target site 93
switches
  cascaded 52
switchShow command 168, 169, 171, 173
symbols in text 15
symbols on equipment 16
synchronous operation mode 34

T

target site
  cabling 71 to 73
  changing prompts at 66
  configuring controllers at 62 to 68
  configuring LUNs 69
  configuring storage at 69 to 71
configuring SWCC agent for AIX 90
configuring SWCC agent for Solaris 99
configuring the host at 74 to 100
connecting controllers and switches 71
connecting host to SAN for AIX 88
connecting host to SAN for NetWare 94
connecting host to SAN for OpenVMS 75
connecting host to SAN for Solaris 97
connecting host to SAN for Tru64 UNIX 78
connecting host to SAN for Windows 91
connecting to external fiber link 73
creating storage units at 69
creating switch zones at 74
disabling access to hosts for AIX 89
disabling access to hosts for Solaris 100
enabling access to hosts for Solaris 99
installing AIX platform kit 83, 126
installing Fibre Channel software for Windows 90
installing HBA driver for NetWare 93
installing HBA driver for Tru64 UNIX 77
installing HBA driver for Windows 90
installing HBAs for AIX 82
installing HBAs for NetWare 93
installing HBAs for OpenVMS 74
installing HBAs for Solaris 96
installing HBAs for Tru64 UNIX 77
installing HBAs for Windows 90
installing multipath software for Windows 91
installing Secure Path agent for NetWare 93
installing Secure Path Fibre Channel HBA device driver for AIX 83, 126
installing Secure Path for Solaris 99
installing Secure Path manager for NetWare 94
installing Solaris platform kit 97
installing SWCC for NetWare 94
installing SWCC for OpenVMS 75
installing SWCC for Tru64 UNIX 78
installing SWCC for Windows 91
multipath software support for Tru64 UNIX 78
renaming host connections for AIX 88
renaming host connections for NetWare 95
renaming host connections for OpenVMS 75
renaming host connections for Solaris 98
renaming host connections for Tru64 UNIX 78
renaming host connections for Windows 92
reverifying disks for Solaris 99
rolling upgrade procedure 228
setting fabric topology 67
setting up AIX at 82
setting up NetWare at 93
setting up OpenVMS at 74
setting up Solaris at 96
setting up Tru64 UNIX at 77
setting up Windows at 90

shutdown upgrade procedure 234
terminal emulator session 212
updating firmware for Windows 90
updating switch zones for AIX 89
updating switch zones for NetWare 96
updating switch zones for OpenVMS 77
updating switch zones for Solaris 98
updating switch zones for Tru64 UNIX 79
updating switch zones for Windows 93
verifying disks for AIX 89
verifying disks for Solaris 99
technical support, HP 17
text symbols 15
troubleshooting
associating HBAs with servers 175
information from controllers 162 to 167
information from operating systems 175 to 178
information from switches 167 to 174
preliminary checks 162
Secure Path 180
World Wide Name ID numbering scheme 164
zoning 180
Tru64 UNIX
connecting host to SAN at initiator site 121
connecting host to SAN at target site 78
enabling access to hosts at initiator site 123
installing HBA driver at initiator site 121
installing HBA driver at target site 77
installing HBAs at initiator site 121
installing HBAs at target site 77
installing SWCC at initiator site 121
installing SWCC at target site 78
multipath software support at initiator site 121
multipath software support at target site 78
renaming host connections at initiator site 122
renaming host connections at target site 78
setting up at initiator site 121
setting up at target site 77
updating switch zones at initiator site 123
updating switch zones at target site 79

U

unplanned failover 43

W

warning
rack stability 17
symbols on equipment 16
web sites
HP storage 17
Windows
connecting host to SAN at initiator site 135
connecting host to SAN at target site 91
installing cluster server 144
installing Fibre Channel software at initiator site 134
installing Fibre Channel software at target site 90
installing HBA driver at initiator site 134
installing HBA driver at target site 90
installing HBAs at initiator site 134
installing HBAs at target site 90
installing multipath software at initiator site 134
installing multipath software at target site 91
installing SWCC at initiator site 135
installing SWCC at target site 91
renaming host connections at initiator site 135
renaming host connections at target site 92
setting up at initiator site 134
setting up at target site 90
updating firmware at target site 90
updating switch zones at initiator site 136
updating switch zones at target site 93
World Wide Name
assigning 64
for HBAs 62
ID numbering scheme 164
location on controller frame 102
location on host bus adapter 46
write history log units
assigning at initiator site 116
creating at initiator site 115
overview 39
performance considerations 41
reaching the end 40
restrictions 40
size considerations 41
switches 41
write history logging 39 to 41

Z

zoneAdd command 208
zoneCreate command 196, 204
zoning
allowing host access between sites 208
creating alias names 190, 193, 195, 201
creating configuration name 196
creating zone names 196, 204
data security 184
hosts and HSG80 subsystems between sites 185
preventing HBA from seeing all active host ports 184
resource partitioning 184
using domain ID and port number 190, 201
zoning a DRM configuration 185 to 208